PENNY M. VENETIS, ESQ.
RUTGERS CONSTITUTIONAL LITIGATION CLINIC
123 Washington Street
Newark, New Jersey 07102
Tel: (973) 353-5687

JOHN McGAHREN, ESQ.
CAROLINE BARTLETT, ESQ.
PATTON BOGGS LLP
The Legal Center
One Riverfront Plaza, 6th Floor
Newark, New Jersey 07102
Tel: (973) 848-5600
Fax: (973) 848-5601
Attorneys for Plaintiffs

ASSEMBLYMAN REED GUSCIORA, STEPHANIE HARRIS, COALITION FOR PEACE ACTION, and NEW JERSEY PEACE ACTION, Plaintiffs, v. JON S. CORZINE, GOVERNOR OF THE STATE OF NEW JERSEY, (in his official capacity) and NINA MITCHELL WELLS, SECRETARY OF STATE OF THE STATE OF NEW JERSEY (in her official capacity), Defendants.	SUPERIOR COURT OF NEW JERSEY LAW DIVISION: MERCER COUNTY DOCKET NO. L-2691-04 CIVIL ACTION

PLAINTIFFS' PROPOSED CONCLUSIONS OF LAW

This document was submitted to the trial court on July 3, 2009. It summarizes all of the evidence presented in the Plaintiffs' case. We firmly believe that it shows that New Jersey's paperless DREs can be hacked easily and made to steal votes. As such, the DREs violate both the NJ Constitution and Title 19 of the New Jersey Statutes.

This document was kept from the public (for over a year) by the Court, pursuant to a request by the New Jersey Attorney General's office. When finally ordered by the Court to justify, legally, on a line-by-line basis, why this document should be kept secret, the Attorney General's office instantly capitulated. The Attorney General's office failed to articulate a single reason why this document should be kept from the public.

The Court subsequently signed an order on October 15, 2010 permitting us to release the entire document to the public.

You may notice that some portions of this document are redacted. Our expert witness, Dr. Roger Johnston, advised us to remove sections of the report concerning his methodology for defeating certain security seals contemplated for use by the State. The removal of this information from the report does not in any way detract from Dr. Johnston's clear conclusions—that the locks and seals contemplated for use by the State of New Jersey do not secure the State's voting machines.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATUTES

OTHER AUTHORITIES

Plaintiffs Assemblyman Reed Gusciora, Stephanie Harris, New Jersey Coalition for Peace Action and New Jersey Peace Action respectfully submit this post-trial memorandum of law in support of each of their causes of action against defendants John Corzine, Governor of the State of New Jersey (in his official capacity), and Nina Mitchell, Secretary of the State of New Jersey (in her official capacity) (collectively, "Defendants").

PRELIMINARY STATEMENT

Paperless DREs have been banned for use not only by most states in this country, but also by legislatures and courts throughout the world. Despite this significant world-wide trend supporting voting integrity, New Jersey lags far behind.

Because of Defendants' failure to follow the law, New Jersey votes are as insecure and subject to manipulation as they were when this lawsuit was filed nearly five years ago. Our State Legislature recognized the need to audit DREs and passed two very strong laws requiring that all voting machines produce voter-verified paper ballots, and that a certain percentage of those paper ballots be hand-counted after each election. Defendants repeatedly failed to comply with these laws, even though both the Appellate Division and this Court have given them every opportunity to do so.

At the direction of the Appellate Division in 2006, this Court held an expedited trial to determine the feasibility of the State's compliance with the voter-verified paper ballot law, and to determine the cost of that compliance. After the trial, the Court concluded that it was highly doubtful that the Defendants could comply with the statute's January 1, 2008 deadline. As such, the Appellate Division instructed this Court to monitor the Defendant's actions to ensure compliance. The Appellate Division also ordered the Court to conduct a full trial on the merits if the Defendants failed to meet the 2008 deadline.

For over two years, this Court held monthly status conferences where the Defendants, and even the Attorney General herself, made repeated representations that they would make the State's voting machines auditable by 2008. That deadline has come and gone, and we are nearing 2010.

It is time for the Court to order the State to replace its insecure and unreliable DREs. At trial, Plaintiffs proved with overwhelming evidence that the Sequoia Advantage Version 9.00H has neither been certified nor thoroughly tested as required by N.J. Stat. Ann. §§ 19:48-1, 19:48-2, 19:53A-3 and § 19:53A-4. Defendants provided no evidence to the contrary. Thus, as a matter of law, these DREs cannot be used in elections in New Jersey.

Moreover, Plaintiffs experts' examination of the 9.00H DREs show that they can be made to steal votes with little effort, and that because of a software bug, they indisputably lost votes in the 2008 Super Tuesday primary election. Plaintiffs' experts' examinations also show that all security measures contemplated by the State are insufficient to secure the State's DREs.

The evidence presented at trial overwhelming demonstrates that the Sequoia Advantage 9.00H is unreliable, inaccurate and that we do not know whether that DRE accurately records our votes. In short, Plaintiffs have proven that the 11,000 Sequoia Advantage 9.00H DREs used throughout this State violate both Title 19 and the New Jersey Constitution.

This Court should immediately decommission those DREs and order the State to replace them with voting systems that comply with the law. Overwhelming scientific evidence shows that the best auditable voting system is the precinct-based optical scanner.

I. THE SEQUOIA ADVANTAGE VERSION 9.00H CANNOT BE USED IN NEW JERSEY ELECTIONS BECAUSE THE SECRETARY OF STATE HAS NOT CERTIFIED THAT DRE.

Under N.J.S.A. § 19:48-2 and § 19:53A-4, before DREs can be certified, they must meet the requirements of § 19:48-1 and § 19:53A-3. Section 19:48-2 states in relevant part that the Secretary of State shall examine all voting machines to ensure that they

> can be safely used by the voters at elections under the conditions prescribed in this subtitle . . . . [T]he Secretary of State shall require the voting machine to be examined by three examiners to be appointed for such purpose by him . . . . Any form of voting machine not so approved cannot be used at any election.

Similarly, N.J. Stat. § 19:53A-4 states that

> No voting device shall be used in an election in this State unless [the machine] . . . meets the requirements in section 3 of this act, and has been approved by the Secretary of State, or other person, agency or board charged with the examination and approval of voting machines. When such device has been approved, any improvement or change which does not impair its accuracy, efficiency, or ability to meet such requirements shall not require a reexamination or reapproval thereof.

Both these sections set out with specificity that the Secretary of State must certify all voting machines. Title 19 does not allow any substitutions for the State's certification process.

The Sequoia Advantage Version 9.00H currently used throughout the State of New Jersey has never been certified and therefore, by statute, cannot be used. N.J.S.A. § 19:48-2 requires the Secretary of State to "examine [a proposed] machine." N.J.S.A. § 19:48-2 also requires a Title 19 Certification Committee consisting of "an expert in patent law" and two mechanical experts, to write a report that will be attached to the Secretary of State's own and presumably separate report.

Only after the Secretary of State has issued a "written report" on a proposed machine, "shall [it] be deemed approved, and machines of its kind may be adopted for use at elections as herein provided." (emphasis added). The Secretary of State has issued no such report for the Sequoia Advantage 9.00H. That is because it was never examined by the Voting Machine Certification Committee.

Throughout this litigation, Plaintiffs have requested all certification reports of all voting machines used in New Jersey. The only certification report that was turned over in discovery for the

Sequoia Advantage is one issued over twenty years ago, in 1987,[1] when Ronald Reagan was President and the Berlin Wall was still standing. "At the time it was designed, which was 1986 and 1987, there were no governmental standards, so it was designed to meet specifications of Sequoia." (Terwilliger Test., 3/30 Trial Tr. at 42:2-4). No other certificates of approval exist for the Sequoia Advantage DRE. We know this to be the case because no post-1987 certifications were presented at trial by Defendants or admitted into evidence. As Mr. Woodbridge, the Chair of the Voting Machine Certification Committee testified, his Committee would never have reviewed the Sequoia Advantage without producing a report. (FOF ¶ 744; Woodbridge Test., 3/4 Trial Tr. at 59:7-9). "[I]f we had five meetings, I can guarantee you we had five reports." (Woodbridge Test., 3/4 Trial Tr. at 59:15-16).

Both Plaintiffs' and Defendants' witnesses agree that the 1987 Sequoia Advantage is a different "kind" of DRE than the Sequoia Advantage 9.00H used today. As documented in Professor Appel's Expert Report, the AVC Advantage has undergone substantial changes since 1987. (FOF ¶¶ 316, 321; Appel Test., 2/5 Trial Tr. at 124:21 to 126:15; Appel Report, §§ 60.1,2,4-12, 63.1, at 130-32, 137.) Professor Appel created a chart of the notable changes made to the different versions of the AVC Advantage:

Version	**Date**	**Notable Added Features**
5.00	1994	multiple ballots
6.00	1995	post-QAT
7.00	1996	expanded option switches; early voting
8.00	1997	dozens or hundreds of bug fixes and minor changes
8.00A	1998	mostly documentation changes
8.00B	1998	bug fix

[1] The Sequoia Advantage DRE 10, which is the only Advantage DRE that supports a voter-verified paper ballot printer is also not certified. Plaintiffs sought declaratory and injunctive relief to prevent this DRE's use. The Court has stayed hearing that motion until resolution of the trial issues. (FOF ¶¶ 848-49.)

9.00	2003	FEC modification requests; audio voting
9.00C	2003	bug fixes; update to FEC coding standards
9.00D, E	2003	
9.00F, G	2004	
9.00H	2005	a few changes related to audio voting and/or FEC requirements
10	?	Daughterboard computer now "main CPU"
10.5	?	Voter-verified paper ballot?

"Different version numbers (e.g., 5.00, 6.00, etc.) of the AVC Advantage are significantly different voting machines that differ in their security, accuracy, and reliability." (FOF ¶ 316; Appel Report § 60.2, at 130; Appel Test., 4/14 Trial Tr. at 59:8-61:1.)

Complete overhauls of the system's hardware have been completed at least twice. Mr. Terwilliger testified that in 1994 "[t]here was a major redesign . . . with a new CPU board." (FOF ¶850; Terwilliger Test., 3/30 Trial Tr. at 21:1-5.) Mr. Terwilliger "was involved and contributed to that redesign." (FOF ¶850; Terwilliger Test. 3/30 Trial Tr. at 21:1-5.) Mr. Terwilliger also testified that "there's been a lot of change to the machine over the years." (Terwilliger Test. 3/30 Trial Tr. at 113:17-18).

The second complete overhaul to the Sequoia Advantage DRE occurred in 2003. From 1984 to 2002, the Z80 motherboard had been the main computer within the Advantage. (FOF ¶ 316.) In 2003, the Advantage was completely modified and a new additional computer was added as a daughterboard in order to allow voting from the audio kit. (FOF ¶ 94.) This change was significant because "[t]he daughterboard processor is much more powerful than the Z80." (Appel Report § 60.7, at 131.) Mr. Terwilliger explained that when the daughterboard was added the "Z80 processor board and its memory did not have the capability . . . enough memory capability to store the audio data." (Terwilliger Test., 3/30 Trial Tr. at 108:12-16). The Z80 processor is very old technology. (Terwilliger Test., 3/30 Trial Tr. at 108:17-20; FOF ¶ 858.)

Changes to the software, firmware, and source code have completely changed the functionality of the AVC Advantage, rendering them entirely different from the 1987 version. (Appel Report, §§ 51.2,5, 61.1-12, 62.1-8, at 106, 132-37; ; FOF ¶ 316.) Mr. Terwilliger, who had "99 percent responsibility for writing the firmware for the [Sequoia Advantage] V2.13 through the V7.0F" could not remember the number of changes made to the Sequoia Advantage over the years because there were so many. (FOF ¶ 850.) The software changes are highly important because software is vital to the DRE. (Smith Test., 3/18 Trial Tr. at 191:19-23; FOF ¶ 850.) In fact, it "defines" the behavior of the AVC Advantage 9.00H and the DRE could not function without it. (FOF ¶ 850.)

Mr. Smith recognized at least 10 changes to the Sequoia Advantage DRE since 1987. (FOF ¶ 316.) Professor Appel found these changes substantial and problematic. "According to comments in the source files, at least one third of the source files were revised, mostly in 2001, to satisfy FEC standards. However, these changes appear to have been done incompletely, and many parts of the source code are in direct violation of the [FEC] standards." (FOF ¶ 827.) These source code changes have made it more difficult to detect vulnerabilities within the voting systems. (FOF ¶ 339; Appel Report, § 51.6-7.)

Defendants' expert testified that when a change is made to the voting system's software or hardware, the whole system must be evaluated to determine if the change will impair the accuracy and reliability of the DRE. Dr. Shamos agrees with Professor Appel that if a new daughterboard or microprocessor is added to a DRE, the whole DRE needs to be re-certified. (Shamos Test., 3/23 Trial Tr. at 203:5-24; FOF ¶ 974.) Dr. Shamos agrees with Professor Appel that just because one version of a DRE has been certified, it does not mean that subsequent versions of the same DRE are also certified. (Shamos Test., 3/23 Trial Tr. at 206:11-14; FOF ¶ 974..)

Dr. Shamos testified that major changes require re-certification by a "state standards review committee." (Shamos Test., 3/25 Trial Tr. at 150:18-25; FOF ¶ 974.). "If there's anything that gets anywhere near the handling of votes or the tabulation of votes, certainly re-certification is needed." (Shamos Test., 3/25 Trial Tr. at 150:18-25; FOF ¶ 974.). Dr. Shamos's beliefs reflect New Jersey law which requires certification for each "kind" of voting machine contemplated for use in New Jersey. No such evaluation or certification of the Sequoia AVC Advantage 9.00H has ever taken place.

Despite significant changes to the AVC Advantage since 1987, the Certification Committee did not conduct any certification hearings for each new version of the AVC Advantage that has been used in the State. (FOF ¶ 772.) No certification was ever issued by the Secretary of State for the 9.00H Sequoia Advantage as is required by N.J.S.A. § 19:48-2. Thus, the "kind" of DRE that is used by over five million voters is not certified. As a matter of law, the 9.00H cannot be used.

This Court should, therefore, immediately decommission all the Sequoia Advantage 9.00H DREs used in the State. This remedy is appropriate, and supported by the evidence discussed above. The Court can decommission the State's DREs with full legal authority, without considering any other evidence that was presented in this case, or that is discussed in Plaintiffs' Conclusions of Law.

II. IF THE COURT DOES NOT IMMEDIATELY DECOMMISSION THE SEQUOIA ADVANTAGE 9.00H, PLAINTIFFS NEED ONLY PROVE THEIR REMAINING STATUTORY CLAIMS BY A PREPONDERANCE OF THE EVIDENCE.

According to statute, the actions of "the Secretary of State in approving [a certified machine] may be reviewed by the Superior Court in a proceeding in lieu of prerogative writ." Although there is a presumption that "a certificate of approval . . . be conclusive evidence that the kind of machine so examined complies with the provisions of" N.J.S.A. § 19:48-1 (emphasis added), that presumption is challengeable and rebuttable. Title 19's plain language makes clear that the presumption of statutory compliance does not even kick in when the "kind of machine" being challenged has never actually been certified.

The evidence discussed in Section I makes clear that the AVC Advantage version 9.00H currently in use is a very different "kind of machine" than the Advantage presented by Sequoia to the Certification Committee in 1987. Subsequent versions of the AVC Advantage have never been presented to the Title 19 Certification Committee for full review. Therefore, the State is not entitled to any presumption that the certificate of approval issued in 1987 is conclusive evidence that the AVC Advantage 9.00H is in compliance with the requirements of § 19:48.

Accordingly, Plaintiffs need only to prove by a preponderance of the evidence that the 9.00H DRE does not comply with Title 19 - See N.J. Evid. R. 101 (b)(1); Liberty Mut. Ins. Co. v. Land, 186 N.J. 163, (2006); see also State v. Seven Thousand Dollars, 136 N.J. 223, 238(1994)("In civil cases, the standard of proof is a preponderance of evidence."); 2 McCORMICK ON EVIDENCE §339 (Strong ed., 5th ed. 1999) (stating that, except "in certain exceptional controversies," the preponderance of evidence standard typically applies in civil cases); accord 9 WIGMORE ON EVIDENCE § 2498 (3d ed. 1940).

The evidence presented by Plaintiffs during five months of trial clearly meets this burden. At a minimum, Plaintiffs have proven by a preponderance of the evidence that the Sequoia Advantage 9.00H DREs and WinEDS tabulation system violate both the New Jersey Constitution and Title 19.

III. PLAINTIFFS HAVE PROVEN THAT THE SEQUOIA ADVANTAGE 9.00H, THE 1987 VERSION OF THE SEQUOIA ADVANTAGE, AND WINEDS SYSTEM CANNOT BE USED IN NEW JERSEY BECAUSE THEY WERE NEVER "THOROUGHLY TESTED."

Before any voting machine can be used in New Jersey, it must be "thoroughly tested" and "reliable." N.J.S.A. 19:48-1a. N.J.S.A. 19:48-1a(a)-(n) enumerates various other criteria that a "thoroughly tested" and "reliable" voting machine must also meet. But, those additional criteria are secondary to the threshold requirement that a voting machine be "thoroughly tested" and "reliable."

The Sequoia Advantage 9.00H does not meet the threshold criteria of 19:48-1a, and thus cannot be used.

A. THE SEQUOIA ADVANTAGE 9.00H DRE HAS NEVER BEEN "THOROUGHLY TESTED" AND THEREFORE CANNOT BE USED IN ELECTIONS.

Pursuant to N.J.S.A. § 19:48-2, any voting machine used in an election must be evaluated by a three-member Committee. The Committee is required to give an opinion to the Secretary of State about whether the voting machines meet the numerous requirements of Title 19. A voting machine can be used only after it has been "thoroughly tested" and the Title 19 Committee produces a report to the Secretary of State reviewing that particular "kind" of machine. N.J.S.A. §§ 19:48-1, 19:48-2.

1. The Sequoia Advantage 9.00H Has Never Been Tested, Let Alone "Thoroughly Tested" as Required by Law.

As discussed in detail in Section I of the Conclusions of Law, there is absolutely no evidence whatsoever that the Sequoia Advantage 9.00H has ever been tested. There is, however, abundant evidence showing that the Sequoia Advantage 9.00H has <u>never</u> been tested. Indeed, since 1987 , there have been at least nine different models of the Sequoia and no fewer than thirteen revisions to the software and source code.

Despite these major changes, at no time was the source code, software, or even the hardware of the multiple models and versions of the AVC Advantage ever analyzed by the Title 19 Voting Machine Certification Committee. Since the Sequoia Advantage 9.00H was never tested, under no interpretation of the statute has the Advantage 9.00H been "thoroughly tested." Thus, by statute, the 9.00H cannot be used.

2. The Sequoia AVC Advantage Model Examined by the Certification Committee in 1987 Was Never "Thoroughly Tested" Either.

a. The 1987 Sequoia Advantage Was Never "Thoroughly Tested" by the Title 19 Certification Committee.

On July 30, 1987, Sequoia presented the Advantage to the Certification Committee for only two hours, from 1:30-3:30 p.m. (FOF ¶ 770.) The Certification Committee 1987 report dated August 5 of that year states that "a similar machine was alleged to have been previously approved by the Secretary of State." As such, the Title 19 Committee assumed that it was reviewing a previously approved DRE. (Ex. P-57.)

The mere fact that the Committee stated that the previous model had been "allegedly" certified is proof that the Committee really had no idea whether the previous model existed. The Committee's report does not identify when the older model was previously certified, the name of this previously certified machine, or the company which manufactured the previously certified machine. (Ex. P-57.) In fact, Mr. Woodbridge, the Committee Chair, could not recall reading any reports concerning the 1987 AVC Advantage's similarity to its predecessor, or conducting any tests to determine whether the 1987 version of the AVC Advantage was in fact similar to its predecessor. (FOF ¶ 768.)

The Title 19 Voting Machine Certification Committee's report shows that Sequoia presented to the Committee a list of eight changes in the AVC Advantage, and asserted that the changes were not significant. (Ex. P-57.) The changes represented to the Committee were as follows:

1. The paging unit was replaced by a full face 250 position ballot.
2. A battery packed cartridge is used in place of an EPROM.
3. The audit trail is placed on the battery backed cartridge instead of on a take up spool.
4. The battery back up power has been increased to six hours.

5. The AVC is now housed in a self-contained booth.

6. A fully developed working demonstrator model (the AVC Companion) has been provided.

7. The candidates names and office titles are now back lit.

8. Special alpha coding has been developed for the results cartridge.

Id.

There is no evidence that the Committee analyzed these changes at all – let alone with any degree of systematic or scientific rigor that would suggest that these DREs should be given a presumption of effectiveness. Instead, the Title 19 Committee merely concluded that "It is evident from the foregoing that the eight (8) basic improvements are not significantly different . . . from the previously approved AVC machine." Id. But, the Committee did not examine the software, the firmware, or source code to make this determination. (FOF ¶ 774.)

Contrary to the Committee's conclusion, the description of at least one update, the "Special alpha coding developed for the results cartridge," strongly suggests that a significant change was made to the software that operates or interacts with the results cartridge. (Ex. P-57.) Since the results cartridge handles vote data, the model should have received a full certification as Dr. Shamos recommended in testimony. As he testified, "[i]f there's anything that gets anywhere near the handling of votes or the tabulation of votes, certainly re-certification is needed." (FOF ¶ 974.) The Committee did not even focus on this software upgrade.

In 1987, the Committee actually expressed some misgivings about the system. The examiners noted that "a member of the public might learn a voter is voting write-in be determining if the voter turns at right angles to the machine to perform the write in [sic] function." (Ex. P-57.) Additionally, the examiners "did not like the ability of the voter to possibly lose or misplace a write-in-ballot." Both of these issues impair a machine's "accuracy, efficiency, or capacity, which the

Committee is charged with protesting." (Ex. P-57.) Despite concerns that the 1987 Advantage did not comply with specific provisions of § 19:48-1a, the Committee recommended that the DRE be certified.

b. The 1987 Sequoia Advantage Was Not Tested by an ITA in 1987 and Its Software Has Never Been Examined by an ITA.

In 1987, "there were no governmental standards," and the AVC Advantage was instead "designed to meet specifications of Sequoia." (Terwilliger Test., 3/30 Trial Tr. at 42:2-4). Mr. Woodbridge testified that he could not remember if any documentation was relied upon in the 1987 Certification. (Woodbridge Test., 3/4 Trial Tr. at 73:1-6). Bob Giles, the director of New Jersey's Division of Elections testified that the members of the Title 19 Committee do not conduct their own research, but instead "rely on the ITAs." (FOF ¶ 704.) Because ITA reports did not exist at that time, no testing of the 1987 Sequoia Advantage ever occurred. (Terwilliger Test., 3/30 Trial Tr. at 42:2-4).

Mr. Terwilliger and Mr. Smith confirmed that the only time that the Sequoia Advantage was examined by an ITA was in 1994 under the 1990 FEC standards. (FOF ¶ 853; Terwilliger Test., 3/30 Trial Tr. at 21:8-17). Defendants own witnesses testified that the 1990 ITA Standards test only hardware, not software (Woodbridge Test. 3/4 Trial Tr. at 43:12-13; FOF ¶ 854). Indeed, Dr. Shamos testified before Congress in 2004 demanding that a new federal voting machine testing system be created from scratch. (FOF ¶ 926.) Dr. Shamos believes the ITA reports are ineffective and arcane–they do not test the installation, implementation, and utilization of DREs. (FOF ¶ 996.)

Defendants' expert also testified that the 1990 FEC standards are obsolete. (FOF ¶ 1602.) The 1990 FEC standards are inadequate for testing DREs because they do not require an examination of a DRE's software and source code to determine if it is flawed. (Shamos 3/23, 192-193:4). Furthermore, the 1990 FEC standards have been fully replace twice by the more stringent standards of 2002 and 2005. But even the 2005 standards do not test for software flaws that may lead to security weaknesses. (FOF ¶ 1009.)

The 1987 Title 19 Certification does not meet the statutory threshold of § 19:48-1a because the Title 19 Committee failed to "thoroughly test" the 1987 AVC Advantage.

B. THE WINEDS SYSTEM HAS NEVER BEEN THOROUGHLY TESTED

Under N.J. Stat § 19:53A-4, the Title 19 Committee has the authority to recommend that a full re-certification hearing is not necessary if, in its opinion, changes made to a voting system that has already been certified do not "impair" the "accuracy" "efficiency" or "ability" of the voting machine to meet the "requirements" of Title 19. N.J.S.A. 19:53. But, the Committee did not test the tabulation upgrades at all, and therefore could not make informed determinations that a full re-certification hearing for the tabulation system was not needed.

1. The Committee Did Not Thoroughly Test The New Vote Tabulation System Introduced By Sequoia in 2005.

On March 2, 2005, the Title 19 Committee conducted a hearing to review an update of the tabulation system for both the Sequoia AVC Advantage and Edge from SQL 6.5 to SQL 2000. (Ex. P-48.) A hearing was held from 10:15-11:00 a.m., lasting only 45 minutes. (Ex. P-48, FOF ¶ 554.) During that short time, the Title 19 Committee determined that a re-certification of the tabulation system used for almost every DRE in the State was unnecessary. (FOF ¶ 773.) Plaintiffs' Exhibit 48 is a sparse two page report in email format, produced only two days after this short hearing, and signed by all three members of the Title 19 Certification Committee.

Mr. Woodbridge testified that Committee reports speak for themselves. (Woodbridge Test., 3/4 Trial Tr. at 73:19-21). In this particular report, Sequoia and the Committee acknowledged that the SQL 2000 upgrade represented a fully "upgraded software system." Furthermore, the report states that the vendor informed the Committee "that SQL 6.5 is no longer supported by Microsoft" and that a full "upgrading to Microsoft SQL 2000" was required. (Woodbridge Test., 3/4 Trial Tr. at 83:5-19).

The Committee report contains no evidence that the Committee conducted any analysis of the changes made to the upgraded software of the tabulation system. (Ex. P-48.) The Committee did not ask Sequoia about the type of testing it performed to ensure that the SQL upgrade would not effect the accuracy of the tabulation systems. (Ex. P-48.) Additionally, there is no evidence that the Committee consulted any computer scientists or computer security experts to determine whether the changes impair the "impair," the "accuracy," "efficiency" or "ability" of the vote tabulation system.

In fact, Mr. Mahoney testified that the Committee did not examine the source code, the software, or conduct any test to see if it contained bugs or was secure. (FOF ¶ 555.) Mr. Woodbridge does not "ever look at the code if [he] can help it." (Woodbridge Test., 3/4 Trial Tr. at 85:1-5; FOF ¶ 1774.) Furthermore, the Committee did not examine any ITA reports regarding the update. (FOF ¶ 776.) Mr. Woodbridge testified that he was unaware of whether an ITA was even available. (FOF ¶ 776.) Shockingly, despite these deficiencies in the Committee's Review, Mr. Woodbridge claimed that the recommendation for certification of the software upgrade "was pretty much a no-brainer." (FOF ¶ 775.)

Instead of conducting its own investigation, the Committee inappropriately relied on Sequoia's interpretation of New Jersey law during the SQL 2000 hearing. "Mr. Woodbridge specifically asked [the vendor] if the changes to the software system would impair the 'accuracy,' efficiency,' or 'ability' of the [voting machines] to meet the 'requirements' of the statute." (Ex. P-48.) Predictably, the Sequoia spokesman answered that the full software upgrade would not impair these statutory thresholds and that a full certification hearing was not needed. (Ex. P-48.) There is no evidence that Sequoia had knowledge of or understood the requirements of N.J.S.A. § 19:53.

(Ex. P-48.) Nonetheless, the Committee "unanimously agreed," based on the vendor's assurances, that the software changes did not require re-certification of the vote tabulation systems. (Ex. P-48.)

The Committee abdicated abdicated its statutory duty when it asked for, and then relied upon the vendor's interpretation of N.J.S.A. 19:53A-4 to conclude that the software did not require a full-review by the Certification Committee. (Ex. P-48.) As such, the Committee did not "thoroughly test" the tabulation system.

2. The Certification Committee Did Not Thoroughly Test The WinEDS System in 2006 Before Determining That A Full Re-Certification Hearing Was Not Necessary.

The Certification Committee substituted vendor representations for its own analysis a second time in 2006 when it again recommended that the WinEDS system be certified without "thoroughly testing" it. (WinEDS Rep., Nov. 14, 2006, 1; Pl. Ex. 50). In 2006, Sequoia upgraded from WinEDS 2.6 to WinEDS 3.0. The upgrade was a completely new version and was a software overhaul of the entire tabulation system (Ex. P-50.) This upgrade gave WinEDS "additional functionality" that would make it part of the "new software and system" to help Sequoia machines manage elections. (Ex. P-50.)

There were 18 items listed by Sequoia as "new in WinEDS 3". (Ex. P-50.) The vendor represented to the Committee that only four of those new items were "relevant" to the systems used in New Jersey. Id. Rather than inquiring why that was the case, the Committee cursorily discussed only the four changes characterized as relevant by Sequoia. (Ex. P-50 at 2-3.) The Committee completely ignored the 14 other changes, even though those 14 features appear to be installed in New Jersey's WinEDS systems.

At the hearing, Sequoia identified and demonstrated four changes in functionality. They include source code and software changes such as: the "ability to filter out absentees from precinct totals;" an Internet connection; a difference in arranging contest and candidate position; a removable results module; a different voice synthesis system; the ability to project results onto a wall or screen; and the requirement that "each time a new module was loaded into the system, the system would . . . have to be refreshed to produce a new output." (Ex. P-50 at 2.) These new functionalities require the installation of new software and directly influence key facets of vote tabulation in the AVC Advantage.

Despite the critical role that WinEDS plays in elections and despite the significant number and quality of the changes to the "new software and system," the Title 19 Committee failed to conduct anything other than a superficial review of the new WinEDS system. Id. This goes against Dr. Shamos' advice that any update that "gets anywhere near the handling of votes or the tabulation of votes" certainly needs re-certification. (FOF ¶ 974.)

Instead of "thoroughly testing" the WinEDS system, the Committee unanimously agreed with the vendor's assertions that a full re-certification hearing was not needed. The Committee failed to explain its basis for concluding that significant changes to the software did not impair the "accuracy, efficiency or ability" of the DRE. (Ex. P-50 at 3.) Notably, the Committee's report does not discuss why the 14 other changes to the tabulation system were not relevant to the hearing.

Alarmingly, the Committee recommended the upgrade for certification even though the upgrade included Internet capability for the WinEDS system. Mr. Mahoney testified that he "has issues" about the WinEDS and Internet capability. (FOF ¶ 559.) In fact, Mr. Mahoney claimed Internet capability was discussed by the Committee because "that was one of [his] biggest things." (FOF ¶ 559.) Also, "[q]uestions were raised by the Committee and the audience with respect to transmitting data over the internet and posslbe interactive vulnerability in directions." (FOF ¶ 559.)

But, the Committee failed to probe into potential attacks and viruses that could infect the voting process from an Internet connection. (FOF ¶ 505.) This lack of attention to potential threats shows that the WinEDS system is not, by any standard, "thoroughly tested" as required by law. Even a minimal evaluation of the Internet feature would have revealed that it most certainly affected the "accuracy," "efficiency," and "ability" of the Sequoia Advantage to meet the statutory requirements to count votes accurately and reliably. Indeed, all witnesses who testified on the effect of Internet connectivity agree that such connectivity irrefutably renders the system insecure. (FOF ¶ 966.)

Just as troubling, the report mentions that, Sequoia fixed "a number of bugs" in the 2006 software. (Pl. Ex. 50.) There is no evidence that the Committee attempted to question Sequoia's representatives about these bugs or their impact on tabulating votes. Id. Notably, the Committee did not find the bugs nor discuss them when it reviewed the WinEDS system a year earlier. The Committee did not consult with computer scientists regarding the WinEDS upgrades. (FOF ¶ 505.) Nor did the Committee examine the WinEDS source code. (FOF ¶¶ 431-35.)

The Title 19 Certification Committee's report on the WinEDS upgrade from version 2.6 to 3.0 merely accepted and relied upon Sequoia's assertions to conclude that the software was acceptable and that it did not require a complete certification hearing. (Pl. Ex. 50). By doing so the Committee failed to "thoroughly test" the WinEDS system, as required by 19:48-1a. As such, New Jersey law prohibits its continued use.

C. MEMBERS OF THE TITLE 19 COMMITTEE APPOINTED TO TEST VOTING MACHINES AND TO RECOMMEND WHETHER THEY SHOULD BE CERTIFIED ARE UNQUALIFIED TO "THOROUGHLY TEST" VOTING MACHINES AND DO NOT "THOROUGHLY TEST" VOTING MACHINES.

1. The Members of the Title 19 Certification Committee are Not Qualified to "Throughly Test" Voting Machines

All 21 counties in New Jersey use DREs. Despite the abundance of outstanding universities within the State (including ones with world-class computer science departments) and the plethora of individuals living in New Jersey with computer science degrees, the Title 19 voting machine Certification Committee consists of three individuals who do not possess the required expertise and knowledge to evaluate our computer-based voting systems. Those individuals are Daryl Mahoney, John Fleming, and Richard Woodbridge.

Title 19 does not require that members of the voting machine Certification Committee possess computer science degrees. This is because the portion of the statute that sets up the Certification Committee was enacted during the Great Depression when computers did not exist. See N.J.S.A. § 19:48-2. But, Title 19 certainly does not prohibit computer scientists from serving on the voting machine Certification Committee. And it is inexplicable, how five years into this lawsuit, given all the scientific evidence that DREs are insecure, Defendants have still not seen it fit to appoint experienced computer scientists and computer security experts to serve on the Committee.

a. The New Jersey Voting Machine Certification Committee Does Not Have the Requisite Skill to "Thoroughly Test" Computer-Based Voting Systems.

For Certification Committee members to determine if a computerized voting system meets Title 19's requirements that it be reliable, accurate, and secure, it is crucial that they possess a strong knowledge of computer science and computer security. Indeed, Defendants' own expert witness, Dr. Shamos, agrees with this point. Dr. Shamos testified each committee member should be "familiar with the computer architectures that are used in these systems. Somebody who is familiar with security vulnerabilities of computer systems. Basically somebody who can take the manual for these machines and understand what's going on, what the software is doing." (FOF ¶ 976.) None of Title 19 Certification Committee members posses these basic skills.

After high school, Mr. Mahoney received some vocational training in auto mechanics but never completed a college degree. (FOF ¶ 513.) Mr. Mahoney "does not know" whether he has ever had any computer or computer software training. (FOF ¶ 515.) Bergen County initially hired him to clean, repair, and reset voting machines as a mechanic. (FOF ¶ 513.)

Bergen County did not use any criteria when selecting Mr. Mahoney for the Certification Committee. (FOF ¶ 543.) Mr. Mahoney took no tests to become a member and in the six years that he has been a member of the Committee, Mr. Mahoney has not received any computer training. (FOF ¶¶ 542-44.) Mr. Mahoney has no knowledge of computer language or programming and only "vaguely" knows the difference between a computer program and a computer operating system. (FOF ¶¶ 542-44.) In fact, during certification hearings, Mr. Mahoney defers to Mr. Fleming for the "computer upgrades and stuff." (Mahoney Test., 2/24 Trial Tr. at 25:5.) Mr. Mahoney bases his decisions regarding whether or not to recommend a voting machine for certification solely on the language of Title 19, the advice of Mr. Fleming, and the statements of vendors. (FOF ¶¶ 546-50.)

Since his appointment to the Certification Committee, Mr. Mahoney has never taken a test to determine whether he should remain on the Committee. (FOF ¶ 543.) No one has ever evaluated his performance, and no supervisor has ever reviewed his certification recommendation decisions. Nobody has ever discussed his performance with him. (FOF ¶ 543.)

John Fleming, another member of the Certification Committee, was assigned to the position in 2001. (FOF ¶ 1052.) He used to be an X-ray technician. (Fleming Test., 4/1 Trial Tr. at 18:12-

13). Currently, he works in the Attorney General's Office. (FOF ¶ 1052.) Mr. Fleming has no formal training in electrical engineering or mechanical engineering. (Fleming Test., 4/1 Trial Tr. at 19:11-16.) He did not major in computer science or computer programming. (FOF ¶ 1054.) He has a B.A. in psychology. (Fleming Test. 4/1 Trial Tr. at 17:18; 23:20-21.) Yet, both Mr. Mahoney and Mr. Woodbridge rely on Mr. Fleming for computer information. (Fleming Test., 4/1 Trial Tr. at 37:4-6.)

The Attorney General's Office assigned Mr. Fleming to the Title 19 Committee without establishing his expertise. (Fleming Test., 4/1 Trial Tr. at 23:20-21.) Mr. Fleming's resume erroneously identifies several operating systems as "computer languages." (Fleming Test., 4/1 Trial Tr. at 19:17-21). Mr. Fleming does not write computer programs, and does not understand the C language–the language of the AVC Advantage 9.00H. (Fleming Test., 4/1 Trial Tr. at 19:19-25, 20:1, 23:5,24-25.) Before he joined the Certification Committee, Mr. Fleming received no training on voting machines. (FOF ¶ 1055.)

The Committee's designated patent lawyer, Mr. Richard Woodbridge, is unqualified to assess the security of the DREs. Mr. Woodbridge has never taken a computer science class. (Woodbridge Test., 3/4 Trial Tr. at 27:11.) He has no experience working in the C language and cannot read it. (Woodbridge Test., 3/4 Trial Tr. at 28:8-10). The last time he worked with computer source codes was decades ago. (FOF ¶ 753.) He is not a computer scientist. (FOF ¶ 752.)

Mr. Woodbridge did not apply to be on the Committee, but was appointed to in 1982 (FOF ¶ 754.) The State of New Jersey conducted no interview to ascertain his fitness for the position. (FOF ¶ 756, 747.) Although Mr. Woodbridge is identified as the Certification Committee Chair, has been on the Committee since 1982, and writes all the Committee's reports, he is not sure of the current wording of the New Jersey Statutes concerning voting machine certification. (Woodbridge Test.

11:25, 12:1, March 4, 2009.)

The Certification Committee members do not have the computer science and computer security background that Defendants' own expert testified is necessary to assess a voting system's security, accuracy, and reliability. (FOF ¶ 976.) Therefore, they do not have the basic skills to fulfill their statutory obligation to "thoroughly test" the voting machine.

b. Certification Committee Members Do Not Consult With Computer Security Experts to Make Up for Their Lack of Ability to "Thoroughly Test" Computer-Based Voting Systems.

Despite the Certification Committee members' lack of knowledge of computer science and computer security, when conducting their evaluations of voting machines, they do not consult with experts who can help them perform their fiduciary obligation to the voters of this State.

Mr. Mahoney testified that the Committee does not consult with any computer scientists or computer security experts and that it does not examine the voting machines' software or source code. (FOF ¶ 548.) Similarly, Mr. Woodbridge, the Committee's Chair, testified that the Committee does not consult with computer scientists before making a certification recommendation. (FOF ¶ 756.) Mr. Woodbridge testified that "[a]s a matter of principle the committee . . . doesn't consult with anybody prior to these meetings." (Woodbridge Test. 3/4 Trial Tr. at 41:25-42:5; FOF ¶ 756). This is because Mr. Woodbridge does not want to be "contaminated by preconceptions of anybody else's opinion." (Woodbridge Test., 3/4 Trial Tr. at 42:4-6; FOF ¶ 754).

Without consulting experts in computer science and computer security, it is impossible for the Committee to "thoroughly test" any voting machine because no one on the Committee has the requisite knowledge to properly evaluate a computer-based voting system.

c. The New Jersey Voting Machine Certification Committee Is Not an Independent Standing Committee With an Institutional Knowledge About Voting Machines.

Mr. Woodbridge testified that there is no "standing committee," (Woodbridge Test., 3/4 Trial Tr. at 6:19-22, 8:2-15) and that Committee members serve from project to project; the make-up of the Committee depends on "who is available" to serve on it on a given day. (FOF ¶ 754.) Mr. Woodbridge describes his participation on the Committee as being "from time to time" and "off and on but not continuously since [1985]." (Woodbridge Test., 3/4 Trial Tr. at 6:9-16.) Since the beginning of Mr. Woodbridge's participation, he estimates that between 12 and 15 people have participated as Certification Committee members (FOF ¶ 754.)

In the past few years Daryl Mahoney, John Fleming, and Richard Woodbridge have regularly served as committee members. Disturbingly, Mr. Mahoney testified that the first time he sat in on the Committee that he had no idea he was a member of the Committee. (FOF ¶ 543.) He was asked by his boss to attend a meeting in Trenton. (Mahoney Test., 2/23 Trial Tr. at 85:13-19). A few days after the meeting, he was asked to sign a report. (Mahoney Test., 2/23 Trial Tr. at 86:9-13). Mr. Mahoney discovered he was a member of the Certification Committee only after he was asked by his boss to attend a second meeting in Trenton. (FOF ¶ 543.)

Because it is not a standing Committee, there is no institutional knowledge concerning the State's voting machines. This problem was present in 1987. (Ex. P-57.) Mr. Woodbridge, then a newly appointed member of the Committee was charged with evaluating the AVC Advantage which "allegedly" had been already certified by the State. Mr. Woodbridge could not remember what documents he reviewed in 1987; and the Committee's report makes no mention of any reliance on previous reports. (FOF ¶ 769.) Mr. Woodbridge admitted that he would only look at old reports "if [he] could find them." (Woodbridge Test., 3/4 Trial Tr. at 68:5-20). Mr. Woodbridge did not know what the Committee reviewed in 1987. He also testified that he did not even know if the Certification Committee even evaluated the Sequoia Advantage 9.00H (FOF ¶¶ 766-68.)

An unbroken chain of knowledge about a particular voting machine is needed to "thoroughly test" it because, as discussed above in detail, vendors continually upgrade their product. Without a complete history of which voting machines are used, and when and why they are upgraded, the Certification Committee cannot determine what steps are needed to "thoroughly test" them to ensure they meet the statutory requirements of reliability, accuracy and security.

2. Besides Being Unqualified, The Members of the Title 19 Committee Have Actually Admitted That They Do Not Actually "Thoroughly Test" Voting Machines.

The Title 19 Certification Committee members have admitted that they do not "thoroughly test" voting machines that they review.

a. The Title 19 Committee Has No Standards To Evaluate Voting Machines, And Uses Only the Plain Language of Title 19 As a Guide

Neither the State nor the Committee have written procedures or guidelines for the Certification Committee to use in determining whether voting machines meet Title 19's requirements. (FOF ¶ 546.) The members of the Certification Committee only "usually have a piece of paper," just a copy of the statute itself, to guide them in their decision-making process. (FOF ¶ 1056.) Mr. Mahoney testified that at the certification hearings, "Mr. Woodbridge reads . . . [the statute] out and we go through it and just say yes, it does or doesn't meet the requirements [of Title 19]." (Mahoney Test., 2/24 Trial Tr. at 24:20.) The statute to which Mr. Mahoney is referring is N.J.S.A. §§ 19:48-1(a)-(b)(1). Those provisions are quoted below to demonstrate that they are skeletal and cannot serve as the sole guide for testing complex computerized voting systems. N.J.S.A. § 19:48-1a reads:

Any thoroughly tested and reliable voting machines may be adopted, rented, purchased or used, which shall be so constructed as to fulfill the following requirements:

(a) It shall secure to the voter secrecy in the act of voting;

(b) It shall provide facilities for such number of office columns, not less than 40 and not exceeding 60, as the purchasing authorities may specify and of as many political parties or organizations, not exceeding nine, as may make nominations, and for or against as many questions, not exceeding 30, as submitted;

(c) It shall, except at primary elections, permit the voter to vote for all the candidates of one party or in part for the candidates of one party or one or more parties;

(d) It shall permit the voter to vote for as many persons for an office as he is lawfully entitled to vote for, but no more;

(e) It shall prevent the voter from voting for the same person more than once for the same office;

(f) It shall permit the voter to vote for or against any question he may have the right to vote on, but no other;

(g) It shall for use in primary elections be so equipped that the election officials can stop a voter from voting for all candidates except those of the voter's party;

(h) It shall correctly register or record and accurately count all votes cast for any and all persons, and for or against any and all questions;

(i) It shall be provided with a "protective counter" or "protective device" whereby any operation of the machine before or after the election will be detected;

(j) It shall be so equipped with such protective devices as shall prevent the operation of the machine after the polls are closed;

(k) It shall be provided with a counter which shall show at all times during an election how many persons have voted;

(l) It shall be provided with a model, illustrating the manner of voting on the machine, suitable for the instruction of voters;

(m) It must permit a voter to vote for any person for any office, except delegates and alternates to national party conventions, whether or not nominated as a candidate by any party or organization by providing an

> > opportunity to indicate such names or name;
> >
> > (n) It shall be equipped with a permanently affixed box or container of sufficient strength, size and security to hold all emergency ballots and pre-punched single-hole envelopes and with a clipboard and a table-top privacy screen;
> >
> > (o) It shall not use mechanical lever machines or punch cards to record votes.
>
> All voting machines used in any election shall be provided with a screen, hood or curtain, which shall be so made and adjusted as to conceal the voter and his action while voting.
>
> It shall also be provided with one device for each party for voting for all the presidential electors of that party by one operation, and a ballot therefore containing only the words "presidential electors for," preceded by the name of that party and followed by the names of the candidates thereof for the offices of President and Vice-President and a registering device therefore which shall register the vote cast for such electors when thus voted collectively.
>
> b. (1) By January 1, 2009, each voting machine shall produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and preserved for later use in any manual audit. In the event of a recount of the results of an election, the voter-verified paper record shall be the official tally in that election. A waiver of the provisions of this paragraph shall be granted by the Secretary of State if the technology to produce a permanent voter-verified paper record for each vote cast is not commercially available.

Using the words of the statute alone to evaluate a complex computer system cannot possibly assist anyone in “thoroughly testing” a proposed voting system.

Both expert witnesses, Professor Appel and Dr. Shamos believe that the certification process should take several days. (FOF ¶ 975.) Exhibits 37, 48 and 50 all clearly demonstrate that the Certification Committee spends less than two hours to evaluate voting machines. Furthermore, the Committee spends very little time deliberating before writing its report for the Secretary of State. Although Mr. Fleming claims the meetings require “[a]s much time as needed until everybody is comfortable,” he also admitted that the Committee spends an average of fifteen minutes determining whether a voting machine should be certified. (FOF ¶ 1058.) Mr. Woodbridge writes the recommendation reports and sends them to the other members by email. (Fleming Test., 4/1 Trial Tr. at 35:19-24). Mr. Mahoney only makes minor modifications, like changing a word or correcting typos, to the report. (FOF ¶ 547.)

It is impossible to tell if all the mandatory enumerated statutory provisions are being met by just reading the statute aloud. The Title 19 Committee's cursory review of the statute is inadequate to "thoroughly test" a voting machine.

b. The Title 19 Committee Does Not Test or Examine Software or Source Code In Any Way

All Title 19 Committee members testified unequivocally that they do not test or examine software or source code. (FOF ¶¶ 548, 757.) Mr. Woodbridge testified, "[s]o the answer is, if we look at the source code or object code, the answer is no." (FOF ¶ 757.) Additionally, the Chair adamantly declared that he does "not want custody of the source code . . . I do not want the responsibility of it." (Woodbridge Test., 3/4 Trial Tr. at 43:1-2).

Generally, from "time to time," the committee may look at ITA reports or reports from Wyle. (Woodbridge Test., 3/4 Trial Tr. at 43:1-5; FOF ¶ 758). However, Mr. Fleming stated ITA reports are mostly "like environmental type stuff and so forth" and do not evaluate software. (Fleming Test., 4/1 Trial Tr. at 28:6-8.) Mr. Woodbridge testified that the Wyle ITA reports have "[h]istorically . . . looked at just the hardware." (FOF ¶ 758).

Without consulting computer scientists and security experts or reviewing a voting machine's source code or software, the Committee cannot discover bugs like the option switch bug (that disenfranchised voters on Super Tuesday in 2008) or the buffer overrun bugs (that can completely disable targeted DREs) or other bugs that Professor Appel testified about. Additionally, without evaluating source code or software, the Committee cannot determine if any vote stealing firmware (like Professor Appel's) is capable of being installed in voting machines being evaluated.

c. The Title 19 Committee Does Not Conduct any Research On Voting Machines It Is Evaluating.

Mr. Woodbridge testified that independent research is not a requirement for the Committee and that the Committee does not go out and "do a lot research." (Woodbridge Test., 3/4 Trial Tr. at 46:10-17). Mr. Woodbridge does not "regularly browse the web to research a proposed machine." (Woodbridge Test., 3/4 Trial Tr. at 46:18-47:8). Mr. Woodbridge was unaware as to whether other members on the Committee conducted research about voting machines. (Woodbridge Test., 3/4 Trial Tr. at 45:22-23). Similarly, Mr Fleming testified: "If you mean do we go out and investigate something, no." (Fleming Test., 4/1 Trial Tr. at 29:14-15.) Mr. Mahoney testified that he does not do any independent research concerning a machine's security. (FOF ¶ 549.)

The Committee has "no staff whatsoever" but members believe they can ask the Secretary of State's office "to get stuff." (Woodbridge Test., 3/4 Trial Tr. at 45:24-46:7). The Committee does not conduct any research to see if voting machines that it is examining have ever been rejected by other states. (FOF ¶ 550, 709, 762.) Although Mr. Woodbridge says that the Certification Committee asks the vendors about voting system de-certifications or pending certifications in other states, the Certification Committee does not do any investigations of its own to verify vendor representations. (FOF ¶ 549-50.) Neither the Director of the New Jersey Division of Elections nor the Certification Committee Chair has thoroughly read the Ohio EVEREST Report and the California Top-to-Bottom Review, which were commissioned by the Ohio and California Secretaries of State, respectively. (FOF ¶ 707). Both studies discuss serious reliability, accuracy and security problems with the WinEDS system and two voting machines used in New Jersey: the Sequoia AVC Edge and the ES&S iVotronic. Mr. Giles testified that there is no one within the Secretary of State's office to conduct research to determine whether other states have decommissioned voting machines used in New Jersey. (FOF ¶ 709.)

d. Reliance On ITA Reports Is Insufficient to "Thoroughly Test" Voting Machines Under New Jersey Law.

Mr. Giles testified that the Committee does not do its own research, "they rely on the ITAs." (FOF ¶ 704.) Mr. Giles, however, does not know whether the reports investigate a voting machine's "hackability." (FOF ¶ 704.)

Title 19 does not mention ITAs. This means that under the statute the State must conduct its own testing of voting machines. While the Secretary of State can choose to consider ITA reports, reliance on them exclusively as testing methods falls short of Title 19's requirement that all voting machines must be "thoroughly tested." This is particularly true, because ITAs do not perform adequate evaluations of voting machines.

ITAs are not federal agencies (FOF ¶ 997.) Dr. Shamos questions the independence of ITAs and has criticized ITA reports for many years. (FOF ¶ 996.) ITAs are paid by vendors, a fact Dr. Shamos believes creates public suspicion, in an opaque testing process that Dr. Shamos believes should be more open. (FOF ¶ 999.) ITAs do not test the installation, implementation, and utilization of DREs. (FOF ¶ 1002.) Dr. Shamos believes the ITA reports are ineffective, arcane and deficient. (FOF ¶ 996.) In fact, before Congress in 2004, Dr. Shamos demanded that a new federal voting machine testing system be created from scratch. (FOF ¶ 996.)

When asked whether there needs to be more federal tests, Dr. Shamos emphatically responded, "[y]es, and the way you would do that is to modify the standards to require more testing. (FOF ¶¶ 996-1006.) Even testing under the current 2002 Federal Standards called the "VSTLs" must be supplemented with additional state testing. States "have to supplement the testing, because if you look at the structure of what the VSTLs are supposed to be doing, they're supposed to be testing things that are of common concern to all the states. They can't possibly get involved in state-by-state individualist requirements." (Shamos Test., 3/23 Trial Tr. at 190:12-17). Dr. Shamos testified that a state's certification process should take several days. (FOF ¶ 975.)

ITAs failed to identify both the option switch bug and the buffer overflow bug in the Sequoia DREs that Professor Appel discovered. (FOF ¶ 993.) They failed to find that a simple vote-stealing program could easily override every single vote-storing mechanism in the AVC Advantage. As such, the Committee's reliance on ITAs to conduct testing is not only misguided but an abdication of the Committee's duties to "thoroughly test" voting machines.

e. The Title 19 Committee Does Not Require That Voting Machines Used in New Jersey be Certified to the 2002 or 2005 FEC Standards.

As discussed above, the AVC Advantage was certified for use in New Jersey in 1987 before any federal testing standards existed (FOF ¶ 995; Terwilliger Test., 3/30 Trial Tr. at 42:2-4). It was used by thousands of New Jersey voters before it went through the certification process in 1994; but even then it was examined only pursuant to the 1990 standards. (FOF ¶ 995.) The 1990 standards test only the hardware and do not test software. Dr. Shamos testified that a voting machine certified to the 1990 standards would "not pass the 2002 guidelines." (FOF ¶¶ 983, 1003.) The 2002 guidelines "are certainly more stringent than the 1990" guidelines. (FOF ¶ 983.) The 2002 guidelines have already been replaced by the more stringent 2005 guidelines. (FOF ¶ 983).

Failure of the Committee to require all voting machines to, at a minimum, meet the most recent and most stringent standards shows that the Certification Committee does not "thoroughly test" voting machines.

f. The Title 19 Committee Does Not Re-Examine DREs Even if Wide-spread Problems With Them are Reported and Known to the Public.

There is nothing in Title 19 that prevents the Committee from requesting that a voting machine be re-examined if problems come to light. Nonetheless, the members of the Title 19

Committee all testified that they see their role as a narrow one, and that they take no action to re-examine a voting machine, even in situations where problems with a voting machine surface and are publicly known.

For example, even after county clerks reported discrepancies in the election results from the 2008 Super Tuesday Presidential Primary Election, the Certification Committee never requested that the Advantage be brought before it to be re-examined. (FOF ¶ 562.) To this day, the option switch bug has not been examined or even considered by the Title 19 Committee to determine if the bug makes the 9.00H DREs unreliable and consequently unfit for use. (See e.g., FOF ¶ 757.) A complete re-examination of the 9.00H is warranted as both Plaintiffs' and Defendants' witnesses agree that voters were disenfranchised by the option switch bug. (FOF ¶ 971, 1015; Terwilliger Test., 3/30 Trial Tr. at 120:13-122:18).

Also shocking is that even after Professor Appel published his detailed analysis of the AVC Advantage 9.00H, the Title 19 Committee did not request that it reevaluate the 9.00H DRE. This is so even though Dr. Shamos testified that election officials should be "very concerned" about Professor Appel's findings. (FOF ¶ 931.)

3. The Director of the NJ Division of Elections is not Qualified to Evaluate Whether the State's DREs are "Thoroughly Tested."

Bob Giles is the Director of New Jersey's Division of Elections. Every county in New Jersey currently uses DREs which are computer based systems. (FOF ¶ 694.) Mr. Giles is not an expert in computer security and does not have any background in computer security at all. (FOF ¶ 694-95.) In fact, he does not have any background in computers. (FOF ¶¶ 693-94.) Outside of writing a simple program for a college class in 1986, Mr. Giles has no experience with computer languages. (FOF ¶ 694.) He cannot understand the source code of the AVC Advantage which is in C language. He does not understand computer programs. (FOF ¶ 694.) Mr. Giles is not trained in electrical or mechanical engineering and cannot fix circuits or computers. (FOF ¶ 694.)

Mr. Giles has no educational background or formal training in computers or DREs. (FOF ¶ 694.) He spent the first eight years of his career working construction jobs. (FOF ¶ 696.) In 1995, he took a job at the Ocean County Board of Elections as an investigator for eight months tracking down individuals whose ballots were returned as undeliverable. (FOF ¶ 697.) Mr. Giles then became the voting machine technician for Ocean County (again for eight months) where he conducted Pre-LAT tests, performed whatever maintenance was required, and delivered Ocean County's optical scan machines to polling places. (FOF ¶ 698-99.) Mr. Giles was then offered the position of assistant supervisor to the Ocean County Board of Elections. (FOF ¶ 698-99.) As assistant supervisor to the Ocean County Board of Elections, Mr. Giles oversaw the day-to-day operations of the office. (FOF ¶ 700.) In May 2008, Mr. Giles was appointed to his current job as Director of the New Jersey Division of Elections. (FOF ¶ 701.)

Due to his extremely limited experience and education relating to computers and electronics, Mr. Giles is unable to understand all of the technical material contained in ITA reports. (FOF ¶ 705.) Quite irresponsibly, Mr. Giles is unsure whether hackability is tested by the ITAs. (FOF ¶ 706.) Despite his responsibilities as Director of the Division of Elections for the State of New Jersey to ensure that voting machines are accurate and secure, Mr. Giles has largely ignored reports published on the insecurities of the Sequoia AVC Edge and the ES&S iVotronics by the States of California and Ohio. (FOF ¶ 702. 707.) He has not read reports by other States concerning Sequoia DREs, does not conduct any research of his own, or require any of his staff or the Title 19 Committee to do so. (FOF ¶ 704, 708-9.) There is no one within the Secretary of States's office who conducts research on voting machines used in New Jersey elections. (FOF ¶ 709.)

Mr. Giles is also responsible for determining whether a voting machine should be re-certified once the vendor has made changes. (FOF ¶ 702.) Mr. Giles does not initiate a hearing on behalf of the State when there is a DRE upgrade, but defers to the vendors to request a re-certification. (FOF ¶ 710.) As discussed above, it is in violation of Title 19 for the state to defer to the vendor, who has an interest in promoting its product and avoiding scrutiny, in determining whether a voting machine or voting machine upgrade should be thoroughly tested.

IV. PLAINTIFFS HAVE PROVEN THAT THE SEQUOIA ADVANTAGE 9.00H AND WINEDS SYSTEM CANNOT BE USED IN NEW JERSEY BECAUSE THEY ARE NOT RELIABLE.

A. THERE IS OVERWHELMING AND UNCONTESTED EVIDENCE SHOWING THAT THE SEQUOIA AVC ADVANTAGE 9.00H IS UNRELIABLE.

1. The Sequoia Advantage 9.00H Is Unreliable Because a Legitimate ROM Chip on the Motherboard Can Be Easily Replaced With a Fraudulent ROM Chip That Makes the DRE Cheat.

The firwmare that controls the Sequoia AVC Advantage 9.00H resides on four ROM chips on the motherboard. (FOF ¶ 76.) Firmware is a computer program, like software, but more or less permanent. (FOF ¶ 74.) Indeed, ROM stands for "Read-Only Memory," and its contents are permanent. (FOF ¶ 67.) Prof. Appel wrote a fraudulent, vote-stealing version of the Sequoia firmware by changing 122 lines of program source code out of approximately 130,000. (FOF ¶ 79.) Then, he wrote the changed part of the firmware to a single ROM chip, using an inexpensive, readily available device called a ROM reader/programmer. (FOF ¶ 79; Ex. P-16.)

This entire process took two weeks; and writing the fraudulent firmware to a ROM chip took about ten seconds. (FOF ¶ 79.) Dr. Shamos agrees that the process of writing a ROM chip takes mere seconds. (FOF ¶ 953.) Once the firmware is written, more fraudulent ROM chips can be rapidly generated in mass quantities to make Sequoia Advantage DREs cheat.[2] (See FOF ¶ 953.)

Prof. Appel demonstrated the process of replacing a legitimate ROM chip on the motherboard of the Sequoia AVC Advantage 9.00H DRE with a vote-stealing ROM chip. The process took him under seven minutes on videotape. (¶ 80). This simple process would pose no difficulties to anyone capable of using a screwdriver. Several ROM chips are in evidence. (EPROM chip, P-13; fraudulent ROM, P-18).

Prof. Appel's physical demonstration consisted simply of picking the lock on the back of the DRE, unscrewing 10 screws on the circuit board cover, popping one of the four legitimate ROM chips out of its socket on the motherboard and replacing it with a ROM containing fraudulent firmware. (FOF ¶ 87b.) After Prof. Appel's demonstrations of the ROM hack, both on video and before this Court, the Advantage 9.00H DRE was permanently altered, and would cheat in every subsequent election. (FOF ¶ 87.) Dr. Shamos agrees that fraudulent firmware could be designed to cheat in subsequent elections. (FOF ¶ 937.)

To demonstrate his vote-stealing program, Prof. Appel ran two full elections. (FOF ¶ 87a.) To demonstrate how the DRE functioned before it was hacked, Prof. Appel first conducted an election as it would be run on a normal election day. (FOF ¶ 87a.) The ballot for Prof. Appel's election was the exact ballot used in the 2008 Democratic Presidential primary. (FOF ¶ 87a.) That ballot was already loaded into the Union County DRE that the State produced for Prof. Appel's team. (FOF ¶ 87.)

The test was simple. Every voter was a Democratic voter, and the voters cast 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (FOF ¶ 87a.) First, Prof. Appel ran a "test"

[2] There are now EPROM chips, Erasable Programmable Read-Only Memory (P-13). However, the general principle is that it requires slightly more effort to rewrite Read-Only Memory than normal memory. (FOF ¶ 68.)

election in Pre-Election Logic and Accuracy Testing, or pre-LAT mode, which is a diagnostic test. (FOF ¶ 87a.) When Pre-LAT mode was finished, Prof. Appel turned off the DRE. (FOF ¶ 87a.) He then turned the DRE back on, and the DRE was in real election mode, where votes were tabulated and stored as official election records. (FOF ¶ 87a.) The DRE properly reported the election results in the test election: 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (FOF ¶ 87a; Ex. P-19 is a handwritten tally of votes case in the Pre-LAT test, and P-20 is the Pre-LAT report printed by the DRE).

Then, in under seven minutes, Prof. Appel replaced the legitimate ROM chip with the ROM chip containing the fraudulent firwmare that he designed. (FOF ¶ 87b.) Dr. Shamos admits that it is possible for unauthorized personnel to replace the ROM chip in the AVC Advantage 9.00H DRE with a fraudulent ROM chip which steals votes, and that this would render the AVC Advantage inaccurate. (FOF ¶ 936.)

Prof. Appel designed the fraudulent firmware on the ROM chip he created to act normally in Pre-LAT mode (to avoid detection), and only to cheat when the DRE was in election mode. (FOF ¶ 81.) Prof. Appel designed the fraudulent firmware to wait until 20 votes have been cast, and then to switch half the votes for the candidate assigned to the H13 button (Bill Richardson) to the candidate assigned to the E13 button (Dennis Kucinich). (FOF ¶ 84.)

Prof. Appel conducted a second full election, identical to the first in all respects, using his fraudulent firmware. (FOF ¶ 87c.) The firmware, as planned, acted normally during Pre-LAT testing, reporting 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (FOF ¶ 87c; Ex. P-20). As designed, the fraudulent firmware was activated when the DRE was in official election mode, transferring half of Bill Richardson's votes to Dennis Kucinich. (FOF ¶ 87c.) Although voters had cast 16 votes for Bill Richardson, and had cast 4 votes for Dennis Kucinich, Prof. Appel's fraudulent firmware stole 8 of Bill Richardon's 16 votes and gave them to Dennis Kucinich. (FOF ¶ 87c.) When the fraudulent firmware added those 8 stolen votes to Dennis Kucinich's 4 actual votes, Kucinich finished with 12 votes. (FOF ¶ 87c.) The final result was 12-8 for Kucinich. Prof. Appel's fraudulent firmware enabled Dennis Kucinich to win an election he had actually lost to Bill Richardson by 16-4. (FOF ¶ 88; Exs. P-19, P-20).

Prof. Appel was able to hack the Sequoia Advantage 9.00H using only common computer science skills, a ROM reader/programmer which cost $149, a ROM chip which retails for $3.87, and a set of lockpicking tools which cost $40. (FOF ¶¶ 67-68, 72; Exs. P-13, P-16, P-17, P-18.) Prof. Appel could have performed his hack using a much cheaper set of tools. (FOF ¶ 72.)

2. The Sequoia Advantage 9.00H is Unreliable Because Anyone with Moderate Computer Skills Can Devise Many Other Ways To Make It Steal Votes.

For purposes of demonstrating the hack in a reasonable amount of time to this Court, Prof. Appel made it wait until the 20th vote was cast. (FOF ¶ 82.) However, it is no more difficult to make fraudulent firmware wait to cheat until after 200 or 500 votes are cast, or to choose any other arbitrary number of votes to wait before cheating. (FOF ¶ 83.)

Prof. Appel also testified that there are many other computer programs he could devise to steal votes. (FOF ¶ 100.) Some examples include:

- Stealing votes as they are cast, reporting to voters that their votes were counted correctly, while actually counting them for another candidate. (FOF ¶ 98.)
- Instead of waiting for a certain number of votes, fraudulent firmware could wait until just before the polls close to steal votes. (FOF ¶ 83.)
- Fraudulent firmware could check what precinct it is in and only cheat if it is in a precinct where the attacker wants to cheat. (FOF ¶ 262.)
- Fraudulent firmware could cheat based on whether a candidate's name appeared to be female or Hispanic, based on the party identification of candidates, or could base its cheating on any information available to it in the information stored in the DRE. (FOF ¶ 97.)

- Fraudulent firmware could also record votes in sequence, allowing corrupt pollworkers to tell who voted for whom, violating ballot secrecy. (FOF ¶ 99.)

These other proposed cheating techniques present no more difficulty than the hack he demonstrated before this Court. (FOF ¶ 100.)

It does not take a programmer of Prof. Appel's skill level to program the simple computer inside the Advantage 9.00H DRE. (FOF ¶ 100.) Dr. Shamos agrees that a person with ordinary computer training could create a vote-stealing program for a Sequoia AVC Advantage DRE. (FOF ¶ 938.) Dr. Shamos also agrees that it is possible to create fraudulent firmware that can evade detection. (FOF ¶ 939.) Dr. Shamos additionally admits that there is no test used by New Jersey to determine that the firmware in an AVC Advantage is legitimate, nor is there any certified device to test ROM chips to see if the firmware on them is legitimate. (FOF ¶ 944.)

Indeed, the Defendants' witnesses unanimously agree that hacking presents a threat to voting machine security in the State of New Jersey. (FOF ¶¶ 842, 845.) Mr. Smith testified that in his prior work for Hart Intercivic, another voting machine manufacturer, that company's voting machines were attacked by technically skilled hackers on multiple occasions. (FOF ¶ 843.) To Mr. Smith's knowledge, none of these hackers were ever caught. (FOF ¶ 844.)

Mr. Terwilliger agrees that fraudulent firmware could avoid detection by Pre-LAT testing. (FOF ¶ 847.) Mr. Smith admitted that Sequoia was aware of the fraudulent firmware problem and chose not to notify New Jersey officials about these weaknesses in the 9.00H DRE. (FOF ¶ 879.) Mr. Smith also admits that Pre-LAT testing is not a tool for detecting fraudulent firmware. (FOF ¶ 879c.)

3. The Sequoia 9.00H is Unreliable Because Hundreds of Thousands of Individuals Possess the Skills to Create Fraudulent Vote-Stealing Firmware in the Form of a Fake Z80 Chip on the Motherboard.

Profs. Appel and Wolf both testified that it is a simple matter to design a processor chip which imitates a legitimate Z80 processor, but contains fraudulent firmware which steals votes much in the same way as Prof. Appel demonstrated with a ROM chip. (FOF ¶¶ 102, 1219.) The imitation Z80 processor would bypass the firmware on the program ROM, and instead run fraudulent vote-stealing firmware. (FOF ¶ 102.) Dr. Shamos agrees that it is possible to do this. (FOF ¶ 957.)

Replacing the Z80 processor on the motherboard is almost as easy as replacing a ROM chip on the motherboard. (FOF ¶ 110.) The only added step is desoldering the Z80 chip from the motherboard and resoldering the fraudulent Z80 chip onto the motherboard. (FOF ¶ 110.) Anyone with a cheap, readily available desoldering tool, soldering iron, and minimal technical skills could easily perform this task. (FOF ¶ 110.) A tool to remove solder can be purchased for $30 or less. (FOF ¶ 111.) The skill needed to desolder and solder a chip to a motherboard is very common in electrical engineering, and in the electronics repair field. (FOF ¶ 110.)

This hack would be more difficult to detect than the program ROM hack, because the program ROM chips would still contain the legitimate firmware. (FOF ¶ 114.) Even if election workers upgraded the firmware by replacing fraudulent or legitimate program ROMs, the fraudulent firmware would still remain on the Z80 CPU. (See FOF ¶ 79.)

There are two main ways of creating a fraudulent Z80 chip. The first, and easiest, is using a cheap, commonly available computer component called a field programmable gate array, or FPGA. (FOF ¶ 1221.) An FPGA is nothing more complex than a device that can be programmed to emulate other chips. (FOF ¶ 105.) An FPGA capable of emulating a Z80 processor is available for $13, and software which can enable it to emulate a Z80 processor is available for free on the Internet. (FOF ¶ 105.) Defendants' witness, Paul Terwilliger, admitted that this is the case, that it is called the "T80 project," and that it is freely available for download from http://www.opencores.org. (FOF ¶ 834.) Further, Dr. Shamos agrees that people have created computer programs to emulate the Z80 processor on hardware other than the Z80. (FOF ¶ 959.)

Prof. Appel testified that it would take a person with the level of skill of a bachelor of science in computer engineering to create a fake Z80 chip with this method. (FOF ¶ 107.) Prof. Wolf, who has designed chips using this method, believed that it would take one of his undergraduate students approximately 56 hours to write firmware to create a fraudulent Z80 chip using this method. (FOF ¶ 1222.) Prof. Wolf testified that a Xilinx FPGA capable of emulating a Z80 is available for a retail price of $15.84 for a single unit. (FOF ¶ 1224.) Casing ranges in price from $8 for a plastic case to $55 for a ceramic case. (FOF ¶ 1232.) These prices come down when one buys in bulk. (FOF ¶ 79.) Prof. Wolf also testified that the per unit cost of mass producing these fraudulent chips and putting them into a plastic case designed to look like a legitimate Z80 processor would be $70 per unit over a run of 500 chips. (FOF ¶ 1232.)

The second way of creating a fraudulent Z80 chip would be to design the chip from the ground up, using VLSI methods[3] commonly available in the computer engineering field. (FOF ¶ 1233.) Such a chip would be absolutely identical in appearance to a legitimate Z80 chip, and literally could not be detected by any practical method. (FOF ¶ 1233.) As the Z80 is a 30 years old chip, its design features are well known to the computer engineering community. (FOF ¶ 1218.) A computer engineer of normal skill would be able to design a completely undetectable fake Z80 chip from the ground up in six months or less. (FOF ¶ 1234.) Prof. Wolf estimated the cost to the attacker as ranging from $640 per unit for a run of 500 units to $80 per unit for a run of 10,000 units. (FOF ¶ 1236.)

[3] VLSI is Very-Large-Scale Integration, a name for the process of creating microprocessors, like the Z80, which use thousands of transistor-based circuits. The technique was more common in the 1970s, when simple processors like the Z80 were state of the art, than now, when microprocessors often contain hundreds of millions of transistors. (FOF ¶ 79.)

4. The Sequoia 9.00H is Unreliable Because Fraudulent Firmware Can Easily Create Redundant, Identical Records Which All Agree, Rendering Fraudulent Election Results Completely Unauditable.

When the Sequoia AVC Advantage 9.00H DRE records a vote, it does so in multiple steps, creating redundant, identical records of the transaction:

- The DRE adds the vote to the audit trail file on the motherboard;
- then, it adds the vote to the candidate totals on the internal memory on the motherboard;
- then, it adds the vote to the audit trail file on the results cartridge;
- finally, it adds the vote to the candidate totals on the results cartridge. (FOF ¶ 89.)

Prof. Appel's fraudulent firmware follows the same pattern, creating four records which all agree with each other. (FOF ¶ 90.) However, the results are fraudulent. (FOF ¶ 91.) Because these four records are the only record of what actually happened in the election, there is no way to verify after the fact that the results are real, rather than the product of fraudulent firmware. (FOF ¶ 92.) There is also no practical way to detect fraudulent firmware. (FOF ¶ 314.)

5. The Sequoia 9.00H is Unreliable Because The Skills Needed to Create and Install Fraudulent Firmware on it are Common.

Plaintiffs' experts, expressing the scientific consensus, made very clear that the experience necessary to create fraudulent firmware for the Sequoia Advantage 9.00H and to install it is common in modern American society. (FOF ¶ 100.)

Prof. Appel testified that picking the locks on the Sequoia AVC Advantage 9.00H is very simple. (FOF ¶ 79.) Despite having no experience picking locks, he was able to learn how to do it in less than a half-hour. (FOF ¶ 72.) Prof. Appel estimated that anyone with a bachelor's degree in computer science or computer engineering would possess the level of skill necessary to create a fraudulent ROM chip. (FOF ¶ 100.) Approximately 25,000 people in the United States earn bachelor of science degrees in computer science. (FOF ¶ 107.) Anyone with a technician's level of skill could perform other phases of the hack, such as replacing a Z80 chip which is soldered onto the motherboard. (FOF ¶ 110.)

Prof. Wolf testified that a senior undergraduate student learning logic design would be capable of designing a fraudulent Z80 chip from the ground up using VLSI methods. This chip would be virtually indistinguishable from the real thing. (FOF ¶ 1233.)

The field programmable gate array, or FPGA method, is even simpler. Prof. Wolf testified that even a junior undergraduate student in the field would be able to design a fraudulent Z80 chip using an FPGA. (FOF ¶ 116 n. 3.) Prof. Wolf estimated that there are half a million people in the world with the computing skills necessary to design and implement a fraudulent Z80 processor.[4] (FOF ¶ 1233.)

Some hacks Prof. Appel testified about require less skill to devise and effectuate. (FOF ¶ 296.) For example, virtually anyone familiar with how normal DOS-based computers operate could write a virus to infect the daughterboard, and anyone with the level of skill of a bachelor's degree in computer science could write a virus to disable AVC Advantage 9.00H DREs selectively. (FOF ¶ 256, 267.)

6. The Sequoia 9.00H is Unreliable Because There Are No Practical Ways to Detect Fraudulent Firmware on ROM Chips or the Z80 Installed on its Motherboard.

a. The State Has No Way to Detect Fraudulent Firmware on the ROM Chip in the Sequoia Adv 9.00H DRE.

Dr. Shamos offered various speculative methods to detect fraudulent firmware, but admitted on cross examination that these would not work on the Sequoia AVC Advantage 9.00H DRE. (Shamos Test., 3/24 Trial Tr. at 62:6-14; Appel Test., 4/16 Trial Tr. at 56:19 to 57:2.) One method suggested by Dr. Shamos is "firmware verification," in which a tester attaches a device to a port on the outside of the DRE, and "dumps" the firmware to compare it to a certified version of the firmware. (Shamos Test., 3/24 Trial Tr. at 62:15 to 64:3.) However, as Dr. Shamos admitted, the Advantage 9.00H DRE does not have such a port, nor could such a port easily be added. (Shamos Test., 3/24 Trial Tr. at 62:15 to 64:3.) Indeed, Dr. Shamos admitted that this port does not exist on any voting machine, and that he knows of no jurisdiction in the United States which uses his firmware verification method. (Shamos Test., 3/24 Trial Tr. at 65:8 to 66:8.)

Dr. Shamos further testified that even opening the DRE and removing the ROM chips physically to test them is not practical, and indeed, could easily be used as a pretext to install fraudulent firmware while pretending to test for it. (See Shamos Test., 3/24 Trial Tr. at 72:15 to 73:9.) Dr. Shamos also testified that this method would not detect a fraudulent Z80 chip, a fraudulent motherboard, or any other form of fraudulent firwmare. (Shamos Test., 3/24 Trial Tr. at 64:4 to 65:7.) Dr. Shamos also admitted that it would not be possible for the tester to determine whether the firmware verification device was, in fact, simply a placebo that was doing nothing. (Shamos Test., 3/24 Trial Tr. at 77:3-22.) In fact, the firmware verification device could actually be rewriting the ROM chip with fraudulent firmware while purporting to test it. (Shamos Test., 3/24 Trial Tr. at 77:8-13.)

Most notably, the State offered no testimony that it ever intends to adopt Dr. Shamos' method of firmware verification.

b. There Are No Practical Ways to Detect a Fraudulent Z80 Processor.

Although they initially claimed that a fake Z80 chip was pure "science fiction," the Sequoia

[4] Embedded computing is when computing devices are embedded into other pieces of hardware for use in real time, like microwaves, automobiles, and electronic voting machines. (FOF ¶ 116 n. 3.)

employees later testified that there were four methods to detect fake Z80s. (FOF ¶ 833, 835.) Prof. Wayne Wolf vehemently disagrees and testified that it is almost impossible to detect a fraudulent Z80 chip. (FOF ¶ 1237.) Dr. Shamos agrees with Prof. Wolf and testified that "you can't easily determine . . . whether you have a very cleverly faked Z80 that has defenses against being detected." (Shamos, Tr., 3/24, 64:13-15.)

Notably, the State presented no testimony that it has any intention of using any of the methods proposed by Smith and Terwilliger to detect fake Z80s.

(i) Visual Examination Does Not Detect Fraudulent Z80 Processors.

The Sequoia employee witnesses claim that one method of detecting fraudulent Z80 chips is simple visual examination. (FOF ¶ 839.) While this would, presumably, detect a blatantly fraudulent FPGA-based Z80 imitation, Profs. Wolf and Appel both testified that there are legitimate companies which will encase an FPGA into any kind of plastic case, including a case identical to that of a normal Z80 processor, in mass quantities at a low per-unit cost. (FOF ¶ 1243.)

The State admits that it has no methodology for visual examination of Z80 processors, or any reason to believe that a well designed fraudulent Z80 processor would have any visible differences from a legitimate Z80 processor. (FOF ¶ 839b.) Even Mr. Smith, a salesman for Sequoia, admitted that there is no reason to believe that there is any difference visible upon naked eye observation between a fraudulent Z80 created using the FPGA method and a legitimate Z80 processor. (FOF ¶ 836.) Mr. Terwilliger, similarly, admits that an FPGA repackaged to mimic a legitimate Z80 processor would be indistinguishable to an ordinary observer. (FOF ¶ 836.)

(ii) X-Ray Analysis is Not Useful for Detecting Fraudulent Z80 Processors.

The Defendants' witnesses proposed a method of attempting to detect fraudulent Z80 microprocessors in Advantage 9.00H DREs by using X-ray analysis. (FOF ¶ 839b.) To use this method, someone would have to remove the motherboard of every DRE to be tested, and take it to a facility with a large X-ray machine. (FOF ¶ 839b.) This method is impractical, ineffective, and costly. (FOF ¶ 1247.)

First and foremost, Prof. Wolf testified that the X-ray would not reveal a well made fraudulent Z-80 chip. (FOF ¶ 1246.) In fact, the actual contents of the chip, which are very small, would only differ at the microscopic level; an X-ray machine would not be able to reveal such detail. (FOF ¶ 1246.)

Secondly, Prof. Wolf testified that the DREs could be damaged in transit or when the motherboards are removed and reinstalled. (FOF ¶ 1247.) Additionally, Prof. Wolf testified that the X-rays could damage or destroy the computer components of the DRE to be tested. (FOF ¶ 1247.) He also testified that removing the motherboard of every DRE in the State to place it into a X-ray machine is clearly impractical. (FOF ¶ 839b.)

Although, Mr. Smith claimed that an X-ray machine could be brought to a voting machine warehouse, these machines are the size of a telephone booth and cost nearly $300,000. (FOF ¶ 839b.) Furthermore, this service is not available from Sequoia and would need to be purchased from a third-party vendor. Mr. Terwilliger admitted in testimony that he is unaware of any manufacturer of portable X-ray machines, and that he has never even seen one. (FOF ¶ 839b.) Prof. Wolf testified that a fraudulent Z80 processor fabricated by the VLSI method to look identical to a normal Z80 processor would not be visible when looking through the X-rays. (FOF ¶ 1256.)

Notably, even legitimate Z80 chips vary considerably in appearance and quality even if they are manufactured by the same company. (FOF ¶ 1237.) Professor Wolf testified that New Jersey 9.00H DREs that were purchased and arrived at the same time in the same shipment might contain slightly different Z80s. (FOF ¶ 1237-42.) Therefore, the X-ray technique would lead to false positives, and could throw the testing process into disarray.

(iii) "Delidding" is Completely Impractical and Even if Implemented, Would Not Successfully Detect Fraudulent Z80 Processors.

Another method proposed by Sequoia employees to detect fraudulent Z80 processors is "delidding." (FOF ¶ 835-36, 839, 1237.) This is a destructive test requiring the dismantling of the DRE and removal of the Z80 chip. (FOF ¶ 1249.) "Delidding" would require the State to open every DRE and de-solder the Z80 processor from the motherboard. (FOF ¶ 1249.) After doing so, the State would then need to deliver the de-soldered Z80 chip to a special facility where skilled testers could examine it more closely. (FOF ¶ 1249.) Mr. Terwilliger explained in that the testing process would require dripping nitric acid onto the chip to dissolve the plastic. (FOF ¶ 835a.)

As Prof. Wolf testified, routinely destroying the microprocessors of all DREs in the State is not a practical detection method. (FOF ¶ 1248.) He also testified that the removal of the Z80 processor could destroy the motherboard. (FOF ¶ 1249.)

Moreover, Prof. Wolf testified that the "delidding" process would still fail to detect a fraudulent Z80 chip designed using traditional VLSI methods. (FOF ¶ 1250.) Mr. Smith essentially agreed with Prof. Wolf's assessment of the "delidding" process. He stated that the "delidding" process would ultimately rely upon naked-eye observations. (FOF ¶ 835a.) Furthermore, Mr. Smith admitted that he is unaware of any State using the "delidding" procedure to test voting machines for fraudulent firmware. (FOF ¶ 839a.)

(iv) Radio Frequency Analysis is Not Demonstrated as a Means of Detecting Fraudulent Z80 Processors, and the State Proposes No Workable Method of Implementing this Method.

The fourth method proposed by Sequoia employees for detecting fraudulent Z80 processors is using radio frequency ("RF") analysis. RF analysis interprets the differentiations of electromagnetic radiation emitted from Z80 processors. (FOF ¶ 835d.) This method would require disassembling the DRE in order to analyze differences between the emissions of a legitimate and fraudulent Z80 processor. (FOF ¶ 1256.)

Prof. Wolf testified that the computer equipment inside the Advantage 9.00H is contained within a "Faraday cage." (FOF ¶ 1256.) This cage is made out of metal and is designed to prevent the DRE from emitting harmful RF radiation. (FOF ¶ 1256.) Therefore, in order to analyze the radio emissions, one would need to open up the DRE and put the emission detection equipment inside the DRE. (FOF ¶ 1256.)

Regardless, Prof. Wolf testified that a fraudulent Z80 processor would appear identical in every respect to a legitimate Z80 processor. (FOF ¶ 1255.) Its radio emissions would not be differentiable. (FOF ¶ 1255.)

Defendants' witness, Mr. Smith, admits that he has never used electromagnetic radiation as a forensic tool and has never detected fraudulent Z80 processors using the RF technique. (FOF ¶ 839c.) Mr. Smith also testified that no State has ever used electromagnetic radiation testing to detect a fraudulent Z80 processor. (FOF ¶ 839c.)

Furthermore, Mr. Smith testified that the vast majority of AVC Advantage 9.00H DRE's electromagnetic radiation emissions do not come from the Z80 Chip. (FOF ¶ 839c.) In fact, the majority of emissions emanate from the wires connecting the chips and the motherboard and not from the CPU. (FOF ¶ 839c.) He offered no testimony as to how the State proposed to isolate the CPU's radiation and test it.

Similarly, Mr. Terwilliger admitted that he does not know what radiation levels are admitted by an FPGA chip–a blank computer chip that can be converted to any type of microprocessor. (FOF

¶ 839c.) Mr. Terwilliger admitted he was unaware of whether any detectable difference between an FPGA chip and a legitimate Z80 processor exists. (FOF ¶ 839c.)

c. Dr. Shamos' Speculative Testing Methods For Detecting Fraudulent Firmware Do Not Exist.

Dr. Shamos proposed a number of speculative methods he claims could be used to detect fraudulent firmware on a program ROM chip or inside the Z80. (FOF ¶ 1019.) None of those methods have been adopted by any State. No evidence was presented that New Jersey is even considering adopting these methods.

Dr. Shamos admitted that all experts agree that software independence is the best method of detecting fraudulent firmware. (FOF ¶ 1033.) He also admitted that all experts agree that software independence is superior to his theoretical methods for detecting vote-stealing software. (FOF ¶ 1032.)

(i) Parallel Testing Does Not Exist As Dr. Shamos Envisions It and Has Not Been Endorsed by any Experts or Adopted by Any States.

Among Dr. Shamos' speculative methods is parallel testing, which Dr. Shamos claims to have invented as a "joke." (FOF ¶ 1020.) Parallel testing requires sequestering a DRE during the course of a day and subjecting it to a scripted voting pattern throughout that day. (FOF ¶ 1021.) Dr. Shamos testified this scripted pattern would be based on the actual patterns of voters. (FOF ¶ 1022.) But he also testified that nobody knows how to determine these patterns. (FOF ¶ 1022.)

Dr. Shamos testified that he has never used parallel testing. (FOF ¶ 1023.) Despite his claim that parallel testing could detect Prof. Appel's fraudulent firmware, Dr. Shamos did not even attempt to use parallel testing to detect Appel's fraudulent firmware. (FOF ¶ 1024.) Dr. Shamos knows that New Jersey does not use parallel testing and he offers no opinion as to whether New Jersey even could implement such a scheme successfully. (FOF ¶ 1025.) Dr. Shamos is unaware of any jurisdictions that use it. (FOF ¶ 1026.)

Dr. Shamos admits that there is no expert community advocating for the use of parallel testing, there is no organized society endorsing it, and no academic journal articles exist supporting its use. (FOF ¶ 1029-31.) In fact, every expert who has actually commented on parallel testing has preferred precinct-count optical scan systems and software independence. (FOF ¶ 1032.) Dr. Shamos also admits that none of the experts he claimed to support parallel testing prefer it to software independence or precinct-count optical scan systems. (FOF ¶ 1033.)

In rebuttal testimony, Prof. Appel testified that he personally spoke to the individuals Dr. Shamos claimed to support parallel testing. (FOF ¶ 407.) All of those individuals stated that parallel testing is inferior to software independence, DREs with voter-verified paper audit trails, and precinct-count optical scanners. (FOF ¶ 407-408.) Further, the Brennan Center for Justice also stated in a published report, read by Prof. Appel into the record, that parallel testing is an inadequate method for protecting the integrity of elections. (FOF ¶ 409.)

Finally, there are easy countermeasures that designers of fraudulent firmware could use to dodge parallel testing. (FOF ¶ 413.) For example, parallel testing, as described by Dr. Shamos, requires extremely time-consuming efforts to simulate entire elections to test on DREs. (FOF ¶ 1021.) Even if New Jersey election workers had the time and ability to perform these complex and lengthy tests, a "secret knock" method could defeat parallel testing. (FOF ¶ 406.) A "secret knock" is fraudulent firmware that only turns on after being given a signal. (FOF ¶ 406.) For example, if a voter, warehouse worker, or a pollworker presses a series of buttons, the fraudulent firmware will activate. (FOF ¶ 406.) The "knock" can be scripted to activate at anytime and can make the DRE either cheat or stop cheating. (FOF ¶ 406.)

(ii) Checkpointing is Another Speculative Testing Method That Does Not Exist.

Dr. Shamos testified that checkpointing could be used to detect fraudulent firmware. (FOF ¶ 1034-35.) But, he also testified that nobody has ever used checkpointing to detect fraudulent firmware. (FOF ¶ 1036.) Dr. Shamos further testified that neither the Advantage 9.00H DRE nor any other DRE can perform checkpointing. (FOF ¶ 1036.)

Dr. Shamos testified that he would be surprised if any jurisdiction actually used checkpointing. He stated that it would be a "real pain" and an "administrative nightmare." (FOF ¶ 1037.) Dr. Shamos testified that to make the Sequoia AVC Advantage 9.00H DRE capable of checkpointing, it would have to be redesigned with new hardware and software. (FOF ¶ 1039.) Accordingly, it would need a full re-certification because it would be a completely new DRE. (FOF ¶ 1039.)

Additionally, election workers would need to be trained to perform the checkpointing at a considerable expense. (FOF ¶ 1041.) Checkpointing, conceptually, requires a multiple time-intensive chores during the course of an election day. (FOF ¶ 1044.) The election worker would need to first, gather vote totals, cast five test votes, count the vote totals, and make sure that they were correctly counted. (FOF ¶ 1044.) Checkpointing would force voters to endure longer lines due to the time needed to interrupt the voting process repeatedly during the day to cast five test votes. (FOF ¶ 1044.)

Dr. Shamos does not even contest Prof. Appel's testimony that checkpointing could be easily defeated by fraudulent firmware. For example, Dr. Shamos' method would require pressing a button on the DRE to test, which would alert the fraudulent firmware that testing was in progress. (FOF ¶ 413.) Just as Prof. Appel's fraudulent firmware does not cheat in Pre-LAT mode to avoid detection, fraudulent firmware could also be designed to recognize and not cheat during checkpointing mode. (FOF ¶ 413.)

(iii) The Prime III Voting Machine Does Not Yet Exist and Uses Software Independence.

Dr. Shamos' Expert Report states that the Prime III voting system would be able to detect Prof. Appel's fraudulent firmware. (FOF ¶ 1045.) However, upon questioning, Dr. Shamos admitted that the Prime III voting system is not a commercially available product and is still in an experimental phase. (FOF ¶ 1046.) Dr. Shamos testified that the Prime III voting machine has not been certified anywhere and that he used the Prime III only once during a demonstration. (FOF ¶ 1049-50.)

More importantly, however, the Prime III Voting Machine is not a paperless DRE. (FOF ¶ 1051.) To the contrary, the Prime III is entirely capable of generating a voter-verified paper audit trail. (FOF ¶ 1051.) Dr. Shamos does not recommend that New Jersey adopt the Prime III voting system. (FOF ¶ 1048.)

7. The Sequoia Advantage 9.00H Daughterboard is Particularly Unreliable.

a. The Daughterboard is Another Computer Inside the DRE.

The Sequoia AVC Advantage 9.00H DRE contains another computer besides the Z80-based computer on the motherboard. (Appel Report § 66.1 at 130; FOF ¶ 858.) In 2003, Sequoia installed a more powerful computer in the DRE. Its purpose was to support audio functions beyond the abilities of the Z80. (Appel Report § 66.2 at 131; FOF ¶ 858.) In sum, Sequoia AVC Advantage 9.00H DRE has two separate but connected computers: an Intel 486-based computer sits on a daughterboard which is plugged into the motherboard containing the Z80 CPU processor. (Appel Report § 60.7.)

The newly added daughterboard is significantly more vulnerable to attack because its firmware is stored in flash memory. (FOF ¶ 233.)

b. The Daughterboard's Use of Flash Memory to Store Firmware is Extremely Insecure and Unreliable.

The daughterboard uses an external cartridge to install audio ballots-- a recorded list of candidates and ballot issues that visually impaired voters listen to in order to cast their votes. (FOF ¶ 232.) However, the same kind of card can be used to replace legitimate firmware on the daughterboard with fraudulent firmware. (FOF ¶ 235.)

If that is done, the fraudulent firmware can infect any legitimate cartridge inserted into the audio ballot cartridge slot and spread the infection further. (FOF ¶ 241.) Simply putting a cartridge containing fraudulent firmware into the audio ballot cartridge will cause the DRE to copy the fraudulent firmware to the flash memory on the daughterboard. (FOF ¶ 240.) Every DRE in the county or the State could become infected by a single corrupted audio ballot cartridge. (FOF ¶ 134.)

Dr. Shamos agrees with Prof. Appel that this is a severe flaw. (FOF ¶ 272.) Similarly, Mr. Terwilliger agrees that flash memory is particularly susceptible to being rewritten. (FOF ¶ 271.)

c. Connecting WinEDS Computers to the Internet Multiplies the Danger of Daughterboard Viruses.

The insecurity of the daughterboard is magnified when combined with the vulnerabilities of WinEDS because viruses can spread between the DREs and the WinEDS computers. (FOF ¶ 230.) A virus could come over the Internet, attack WinEDS computers, and spread to DREs. (FOF ¶ 230.) An innocent election worker performing routine duties can just as easily (but inadvertently) spread the infection as a corrupt election worker. (FOF ¶ 237.) The mere physical act of inserting a cartridge into a WinEDS computer or Advantage 9.00H DRE spreads the virus. (FOF ¶ 235.) If either the WinEDS computer, the DRE, or the cartridge are infected, the infection will spread. (FOF ¶ 238-41.)

This automatic copying mechanism is not selective. It will spread fraudulent firmware deliberately created in order to steal votes. (FOF ¶ 235.) It will also spread viruses inadvertently caught from the Internet. (FOF ¶ 230.)

Dr. Shamos agrees with Prof. Appel that WinEDS computers should never be connected to the Internet. (FOF ¶ 966.) Even the Sequoia employee witnesses, Smith and Terwilliger, agree that this should never occur. (FOF ¶ 866.) However, the Internet files on the Union County laptop prove that WinEDS computers are frequently connected to the Internet, even on election days. (FOF ¶ 210.)

This is not an isolated occurrence. Mr. Mahoney (Bergen County), Ms. Gentile (Hudson County), and Ms. Sollami-Covello (Mercer County) all gave testimony that WinEDS computers in their counties are connected to the Internet. (FOF ¶ 524, 490, 577.) Moreover, Mr. Giles testified that there is no State policy requiring that voting systems not be connected to the Internet. (FOF ¶ 722.)

Because the daughterboard is used to tabulate the votes of the visually impaired, those votes are especially vulnerable to theft. Fraudulent firmware can alter the votes of the visually impaired, and transmit the fraudulent results to the motherboard, with no way ever to determine what the voters' actual intentions were.

Viruses or fraudulent firmware in the daughterboard can also affect all voters. Viruses can cause the entire DRE to shut down. This can lead to long lines or even chaos on election day.

d. The Advantage D-10 is Completely Without Defense Against Vote-Stealing Viruses and Tampering Because the Daughterboard as the Main Computer.

In the AVC Advantage 10 DRE, Sequoia moved most of the DRE's functionality to the daughterboard. (FOF ¶ 858.) Thus, in the D-10 the daughterboard is the main computer for the DRE and reducing the motherboard is reduced to a mere appendage. (FOF ¶ 858.) Mr. Terwilliger admits that if he were to design a DRE anew, it would not be the D-10. (FOF ¶ 858.)

The daughterboard of the 9.00H DRE is susceptible to vote-stealing viral infection. (FOF ¶ 233.) It mostly handles the votes of visually impaired voters. (FOF ¶ 233.) But, in the AVC Advantage 10, the same insecurities affecting the votes of the visually impaired will threaten all voters. Even Defendants' expert, Dr. Shamos, believed that this defect was extremely severe and required immediate remediation. (FOF ¶ 961.)

Making this extremely insecure daughterboard computer the main computer in the Advantage 10 DRE allows an attacker to steal everyone's votes and not just the votes of the blind. (FOF ¶ 272.)

8. Even When Operated as Intended, the Sequoia AVC Advantage DRE is Unreliable.

a. The Option-Switch Bug Has Disenfranchised New Jersey Primary Voters.

On Super Tuesday, February 5, 2008, at least 37 Advantage 9.00H DREs malfunctioned in eight counties. This disenfranchised voters. (FOF ¶ 340.) It also illegally allowed voters to cast votes in the primary election of the party in which they were not registered to vote. (FOF ¶ 340.)

The first clue to the existence of this bug appeared after the close of elections on February 5, 2008, when Joanne Rajoppi, the Union County Clerk, noticed that the results tape data and the summary report data did not completely agree, in at least nine districts in Union County which use the Advantage 9.00H DRE. (FOF ¶ 625-626.) Further, in five of the nine districts, there were fewer voter authority slips than votes on the results cartridge, meaning more votes were cast than there were voters. (FOF ¶ 629.)

As a result of the option-switch bug, vote totals for each party disagree with the candidate total figures. For example, in Union County, one DRE reported 361 votes for Democratic candidates, but reported that 362 Democratic voters had cast a vote. (FOF ¶ 346.) The same DRE reported 61 total votes for Republican candidates, but reported that 60 Republican votes had been cast. (FOF ¶ 347.) Both these results should be impossible. (FOF ¶ 346-47.)

The ballot definition file for the February 5, 2008 primary requires that each voter cast exactly one vote for a candidate of the voter's party. (FOF ¶ 346-47.) It should be impossible for: a) a voter to fail to cast a vote in the primary election; and b) to vote for someone in the opposite party. (FOF ¶ 346-47.)

Ms. Rajoppi was not alone in noticing that the results reports printouts from the Advantage 9.00H DREs were clearly erroneous. (FOF ¶ 586.) Paula Sollami-Covello, the Mercer County Clerk, also inspected the results reports printouts from the Advantage 9.00H DREs, and noticed the same erroneous results. (FOF ¶ 587-90.) For the February 5, 2008 Presidential primary, the results reports from 30 Sequoia AVC Advantage 9.00H DREs disagreed with the results cartridges from the same election. (FOF ¶ 590.) On 30 DREs, there were more votes than voters. (FOF ¶ 591.) On 27 of those DREs, the number of overvotes for one party equaled the undervotes for the other party. (FOF ¶ 592.) Voters who were registered Republicans had been presented with the Democratic slate of candidates, and vice versa. (FOF ¶ 593.) Multiple Democrats attempted to write-in "Hillary Clinton" in the Republican primary. (FOF ¶ 594.) These votes were not counted, because Democratic voters may not vote in the Republican primary. (FOF ¶ 595.)

Prof. Appel subsequently found that the "option-switch" bug causes the Advantage 9.00H's to behave incorrectly when a pollworker (accidentally or deliberately) presses a button on the operator panel of the DRE while activating the voting machine for a primary election. (FOF ¶ 346.) When the bug is triggered, the "option switch" for the voter's party, is correctly activated. The "option switch" counts how many voters for each party used the DRE during the election. (FOF ¶

341.) However, the DRE will not allow a voter to vote in the correct party primary. (FOF ¶ 341.) Instead, the bug causes the DRE to activate the slate of candidates for the other party. (FOF ¶ 341.) So, in violation of State law, a Republican is allowed to vote for a Democratic candidate in the Democratic primary, and vice versa. (FOF ¶ 342.)

Witnesses on both sides, including Dr. Shamos, agree that this is a serious problem which disenfranchised voters on Super Tuesday, and that it could be exploited to disenfranchise voters. (FOF ¶ 971.) As Dr. Shamos simply stated, "it's bad." (FOF ¶ 1051.)

The option-switch bug makes the DRE unreliable because voters are prevented from voting in their party's primary, and they are permitted to vote in the opposite party's primary. (FOF ¶ 341.) This also violates N.J.S.A. § 19:23-45 (requiring that voters in primary elections be allowed to cast vote in their party and no other).

b. County Clerks and Other Constitutional Officers Doubt the Reliability of the Sequoia Advantage and the Validity of the 2008 Presidential Primary.

Because of the option-switch bug, Union County Clerk Joanne Rajoppi did not certify the result of the election in the usual way. (FOF ¶ 630.) Instead, she expressed reservations about the AVC Advantage's reliability, because she "could not swear that it was accurate." (FOF ¶ 635.) Ms. Rajoppi tried to contact the Attorney General's office three to four times over the course of a month, and spoke to different individuals about the option-switch bug, including Donna Kelly or someone in Donna Kelly's office. (FOF ¶ 631.) The Attorney General's office never even bothered to contact Ms. Rajoppi. (FOF ¶ 632.) Ms. Rajoppi also attempted to contact Sequoia to discuss her concerns about the reliability of the Sequoia Advantage. (FOF ¶ 633.) Those attempts were also rebuffed. (FOF ¶ 633.)

Similarly, Ms. Sollami-Covello, the Mercer County Clerk, attempted to contact a number of

State officials, including Donna Kelly. (FOF ¶ 600.) The Attorney General's office failed to respond to Ms. Sollami-Covello. (FOF ¶ 601.) Ms. Sollami-Covello also contacted Joe McIntyre of Sequoia. (FOF ¶ 603.) Sequoia's only response was a press release attempting to explain the error. (FOF ¶ 603.)

Ms. Rajoppi testified that she experienced additional problems with the Advantage DRE since she discovered the option-switch bug. (FOF ¶ 696.) In particular, she received many complaints from members of the public, including the Mayor of Springfield, about the behavior of the Sequoia AVC Advantage 9.00H DREs in the November 2008 general election. (FOF ¶ 696.) The voting machine also rejected an Hispanic candidate's name in the June 2008 primary election. (FOF ¶ 876.)

As a result, Ms. Rajoppi has been hindered from carrying out her duties under the New Jersey Constitution. (FOF ¶ 644.) While she continues to certify elections, she harbors grave doubts about the reliability and accuracy of the results reported by the 9.00H DREs. (FOF ¶ 644.)

Ms. Rajoppi is far from alone in her concerns about the unreliability and inaccuracy of the Sequoia AVC Advantage 9.00H DREs. (FOF ¶ 638.) The Constitutional Officers Association, a New Jersey organization of elected State constitutional officers such as Sheriffs, County Clerks, Surrogates and Registers of Deeds and Mortgages, passed a resolution calling for an independent investigation of the inaccurate election results produced by the Advantage 9.00H DREs. (FOF ¶ 638.) The Association then conveyed this sentiment via formal letter to the Attorney General's office. (FOF ¶ 638.) Ms. Rajoppi also attempted to retain Prof. Felten of Princeton to investigate the unreliable 9.00H DREs further. (FOF ¶ 641.) Rather than assist the attempt to investigate, the Office of the Attorney General, including Donna Kelly, discouraged Ms. Rajoppi from proceeding. (FOF ¶ 643.)

c. Protections Against The Option-Switch Bug Have not Been Adequately Addressed by the State or Sequoia.

Despite the abundant evidence that the option-switch bug is a real problem, the State has done little to remediate it. (FOF ¶ 869-871.) Sequoia's Mr. Smith, testified that even he believes the option-switch bug is "a real problem." (FOF ¶ 869.) Sequoia's Mr. Terwilliger testified that Sequoia has taken no action to remediate the option-switch bug in the Advantage 9.00H DREs used in New Jersey. (FOF ¶ 871.)

Another State witness, Mr. Clayton, testified that Sequoia's proffered "solution" to this software bug is to attach a piece of plastic to the DRE with velcro in an attempt to prevent pollworkers from pressing the buttons which trigger the bug. (FOF ¶ 872.) This underscores the State's Band-Aid approach to deep, systemic problems.

This solution is not enough and does nothing to remedy the unreliability caused by the option switch bug. Mr. Clayton testified that there is no protocol to ensure that this plastic shield is actually on the Advantage 9.00H DREs when they are in use. (FOF ¶ 679.) Mr. Smith testified that this piece of plastic was the only attempt made to remediate the option-switch bug. (FOF ¶ 871.) A piece of plastic attached by velcro clearly does not prevent pollworkers from inadvertently or purposely triggering the bug. Moreover, there is no protocol in place to let pollworkers know to keep the piece of plastic in place. (FOF ¶ 679.)

9. Many Other Bugs and Sloppy Software Practices Likely to Cause Bugs Make the Sequoia Advantage 9.00H Unreliable.

a. The Buffer Overrun Bug Can Shut Down the Advantage.

Another bug Prof. Appel discovered is the buffer overrun bug. That bug commonly occurs in badly written software. (FOF ¶ 263.) A buffer overrun bug occurs when software allows ill-formed input to cause unexpected results. (FOF ¶ 263.) Sequoia's buffer overrun bug, described in

Appendix B of Prof. Appel's report, allows the DRE to be completely disabled by a virus on the daughterboard. (FOF ¶ 263.) Effectively, the daughterboard sends a malformed message to the motherboard, causing the DRE to enter an endless cycle of resetting itself. (FOF ¶ 264.)

Dr. Shamos agrees that the buffer overrun bug which allows the daughterboard to cause the Advantage 9.00H DRE to crash is a serious error which needs to be remediated immediately. (FOF ¶ 272.) Dr. Shamos further agrees that because of the insecurity of WinEDS and the daughterboard, an attacker does not need even to get near to the Advantage 9.00H DRE to infect it with a virus. (FOF ¶ 274.)

b. Known Sloppy Practices and Bugs Make it More Likely That There Are More Bugs in the 9.00H.

The Advantage 9.00H source code reveals that the 9.00H firmware is likely to contain more bugs. (FOF ¶ 322.) Because of the limited amount of time and the necessity to explain known bugs and demonstrate fraudulent firmware, Prof. Appel and his team were unable to examine the source code exhaustively for more bugs. (FOF ¶ 338.)

However, even if Prof. Appel and his team had the time for an exhaustive examination of the 130,000 lines of source code, they would still not be sure that they detected all the bugs, or even fraudulent firmware. (FOF ¶ 338.) This is because there is software running in the Advantage for which Sequoia claims it does not have source code. This means that Sequoia has no idea what is actually running in the AVC Advantage 9.00H. (FOF ¶ 339.) This fails to meet the standard of New Jersey law, which requires that a voting machine be "thoroughly tested" and "reliable." N.J.S.A. 19:48-1. One cannot test what one does not even know exists.

Defendants' witness, Mr. Smith, admits that the Advantage 9.00H DRE contains software from third-party vendors which is not independently tested by Sequoia. (FOF ¶ 863.) Mr. Smith does not know which vendors provide that software, but stated that he believes, but is not certain, that in addition to software from Microsoft and Datalight, one of the vendors has the word "General" in its name. (FOF ¶ 863.)

Even without Sequoia's disturbing admission that it does not know what software is running in the Sequoia AVC Advantage 9.00H, the sloppy software practices embodied in the 9.00H's source code cast grave doubt on the security and reliability of the Advantage. (FOF ¶ 322.) In addition to using an obsolete version of the C programming language, which cannot be tested with modern error detection tools, Sequoia's source code is a confusing mess which is very difficult for subsequent programmers to understand and fix when the DRE misbehaves. (FOF ¶ 320.) This deficient software is also, as a result, more vulnerable to attack. (FOF ¶ 322.) Dr. Shamos admits that Sequoia's software development practices in designing the Advantage 9.00H DRE were poor. (FOF ¶ 968.)

These poor practices, as a whole, weaken the integrity of the entire voting system and make it unreliable. (FOF ¶ 322.) We do not know the full extent of the unreliability.

10. The Sequoia AVC Advantage 9.00H is Unreliable Because it Falsely Tells Voters that Votes Are Recorded When They Are Not.

The AVC Advantage 9.00H user interface is deeply flawed, and issues confusing, misleading, or outright false messages to the voter. (FOF ¶ 357.) One of the worst of these flaws is that it falsely indicates to the voter that a vote has been counted when the machine is not activated and not counting votes. (FOF ¶ 353.)

Even when the AVC Advantage 9.00H is not activated and cannot count votes, the DRE gives multiple false indications to the voter that a vote has been counted. (FOF ¶ 353.)

For example:

- the DRE lights the green X by a candidate's name when the button for that candidate is pressed;

- the Cast Vote button lights up when it is pressed;
- and the LCD panel displays the message “VOTE RECORDED THANK YOU,” just as if a vote had been cast. (FOF ¶ 353.)

Whether the pollworker fails to activate the DRE accidentally or deliberately, voters seeing the signals listed above could very well be tricked into losing their votes. (FOF ¶ 354.)

The option-switch bug, discussed above, is another way that the DRE gives false signals to a voter that she has voted, when in reality, she has not. If a pollworker, either inadvertently or maliciously, presses a button on the operator panel after activating the DRE, but before a voter casts a vote, it will silently deactivate the DRE. (FOF ¶ 365.) The vote will not be counted. (FOF ¶ 366.) However, the DRE will give multiple indications to the voter that a vote has been counted, including the false “VOTE RECORDED THANK YOU” message on the LCD panel. (FOF ¶ 353.)

These user interface design flaws are not simply theoretical concerns. Plaintiff Stephanie Harris testified that the first time she attempted to vote on a Sequoia AVC Advantage DRE, she chose her candidates, pressed the “CAST VOTE” button, and exited the voting booth. (FOF ¶¶ 4-6.) A pollworker informed her that her vote was not counted, and requested that she try to vote a second time. (FOF ¶¶ 7-8.) This sequence of events repeated two more times. (FOF ¶¶ 9-10.) The last time, the pollworker told Ms. Harris that he thought the DRE registered her vote. (FOF ¶¶ 9-10.)

Neither the pollworker nor Ms. Harris had any means to be certain that Ms. Harris’ vote actually was cast. (FOF ¶¶ 10.) Ms. Harris testified that since then, she cannot rely on Sequoia AVC Advantage DREs to count her votes correctly. (FOF ¶¶ 12.) Dr. Shamos agrees that the user interface of the AVC Advantage 9.00H DRE is poorly designed in many ways and that “the vendor should be compelled to produce a better interface[.]” (Shamos Rebuttal, ¶ 123, at 28.)

11. The Sequoia 9.00H is Unreliable Because Its Flawed User Interface Can Confuse Voters and Cause Lost Votes.

The primitive buttons-and-lights user interface of the Sequoia AVC Advantage 9.00H DRE can easily cause votes to be lost. (FOF ¶ 357.)

For example, even when the DRE is not activated, it will light up a green X next to the name of a candidate when the voter presses that button. (FOF ¶ 359.) This falsely conveys to the voter that she has properly selected the candidate of her choice. (FOF ¶ 359.) Dr. Shamos agrees that this behavior is "confusing and risky." (FOF ¶ 360.) Sequoia has been aware of this problem since 2006, but has not fixed it. (FOF ¶ 360.) If the voting machine is not activated, it should not indicate that it is. Any deviation from this common sense principle is evidence of unreliability.

Another problem with the user interface is that it fails to warn voters that they have failed to cast votes for offices or ballot questions for which they are entitled to vote. (FOF ¶ 970.) The buttons and lights interface allows no practical way for the DRE to communicate a message about an undervote. Dr. Shamos agrees that this feature is problematic. (FOF ¶ 970.) Studies show that this feature on the Advantage has a disproportionate effect on minority voters.[5] (FOF ¶ 375.)

12. The Sequoia AVC Advantage 9.00H Is Unreliable Because It Does Not Allow a Voter to Undo a Write-In Vote, Violating Federal Guidelines.

The Advantage 9.00H DRE provides no means to undo a write-in vote. (FOF ¶ 382.) After the voter has used the keypad to enter the name of a candidate, the write-in cannot be unselected. (FOF ¶ 382.) This makes the DRE unreliable because a voter is given no warning about this feature. (FOF ¶ 382.) A voter may take a different approach if she is made aware that she cannot change her

[5] Empirical studies have, indeed, shown that elections using the AVC Advantage 9.00H have an unusually large number of undervotes. David Kimball, Voting Equipment and Residual Votes on Ballot Initiatives: The 2006 Election in New Jersey, David Kimball (Feb. 2007), available at http://www.umsl.edu/~kimballd/NJ06resid.pdf. (FOF ¶ 375.)

vote. (FOF ¶ 382.)

The inability to change a write-in vote is also a violation of the FEC Guidelines for voting machines, which say: "A means for correcting a vote response should be readily available. For non-paper based systems, this should be built into the design of the system." (FOF ¶ 353; Appel Report, § 36.2, at 86; VVS 2002, App. C, sec. C.8(e).) Dr. Shamos agrees that the law requires that the Advantage 9.00H DRE allow the voter to correct a write-in vote, but that it does not do so. (FOF ¶ 972.)

The result of this design flaw is that these voters are more likely to be disenfranchised because they are unable to cast their desired votes. (FOF ¶ 376.)

13. The Sequoia 9.00H is Unreliable Because it Gives Voters Confusing Audio Signals.

The chirping sound the Advantage 9.00H makes to indicate activation is the same as the sound that the Advantage makes when a vote is cast. (FOF ¶ 373.) Thus, it is difficult for even an observant poll worker or voter to tell what the sound means. (FOF ¶ 373.) This is especially true in a noisy, busy environment. (FOF ¶ 373.) Even in optimal circumstances, though, the chirping sound is barely audible. (FOF ¶ 373.)

Further, it is troubling that there is no sound to indicate the DRE has been deactivated either deliberately or inadvertently by pollworker error. (FOF ¶ 374.) This means that even attentive voters, who listen for the chirping sound before they enter the voting booth to ensure that the voting machine is activated, may still be tricked. (FOF ¶ 374.) The DRE will make no sound if the pollworker deactivates it before the voter has entered the voting booth.

It is easy to trick a voter in this way because the DRE will still give numerous false indications that the DRE has counted their vote, compounding the problem. (FOF ¶¶ 365-67.) Dr. Shamos agrees that the Advantage 9.00H gives voters insufficient information to determine if the

DRE is activated and counting votes. (FOF ¶ 969.) He also testified that this lack of information could lead voters to believe they are voting when, in fact, they are interacting with a deactivated DRE which is not counting their votes. (FOF ¶ 969.)

14. Prof. Appel Discussed Other Serious Flaws in the Sequoia AVC Advantage 9.00H DRE that Make it Unreliable.

The list of flaws Prof. Appel detailed in his expert report and in his testimony before this Court is long and meticulously detailed. (FOF ¶ 36.) Some other problems which make the Sequoia AVC Advantage 9.00H DRE unreliable include:

- Manipulation of ballot definition files can reverse buttons for candidates or give two votes to a candidate with every single button press for that candidate. (FOF ¶ 225.)
- Manipulation of results cartridges by a variety of means can corrupt the records of elections. (FOF ¶ 93.)
- The Advantage 9.00H DRE does not give adequate warning to the voter about undervotes, or failing to cast a vote for all races and questions for which the voter is eligible. (FOF ¶ 970.)
- Vote data is not electronically authenticated by modern, well known methods to detect whether they have been altered. (FOF ¶ 310.)

Dr. Shamos agrees that Prof. Appel's examination of DREs in New Jersey is essential to their security. (FOF ¶ 930.) Further, he testified that "everybody in the voting field should be concerned about Professor Appel's findings." (FOF ¶ 931.) Dr. Shamos agrees that there are problems with Sequoia's voting software and physical security, and that the AVC Advantage 9.00H in particular has "serious vulnerabilities." (FOF ¶ 932.) Dr. Shamos agrees these problems need to be remedied. (FOF ¶ 934.)

B. THE SEQUOIA ADVANTAGE WINEDS VOTE TABULATING SYSTEM IS NOT RELIABLE.

1. The WinEDS System is Unreliable Because it Cannot Ascertain Whether DREs Have Been Corrupted.

As Prof. Appel demonstrated, when fraudulent firmware steals votes, it writes the fraudulent results it creates to four places. (FOF ¶ 90.) Vote totals are written to the results cartridge and the memory on the motherboard, and ballot images, the so-called "audit trail," are also written to the results cartridge and the memory on the motherboard. (FOF ¶ 90.) The results cartridge is used to transfer vote totals from precincts to county offices to be totaled by the WinEDS software. (FOF ¶ 224.)

The Sequoia AVC Advantage 9.00H DRE and the WinEDS software used to tabulate votes after an election do not have any method of authenticating the data from results cartridges to ensure that they are not the product of fraudulent firmware. (FOF ¶ 314.) Similarly, if results cartridges are altered in transit, the WinEDS computer cannot detect that fraud. (FOF ¶ 312.) Indeed, when confronted with a results cartridge loaded with fraudulent data, the WinEDS computer will accept it without question and tabulate it just as it would legitimate data from a results cartridge. (FOF ¶ 93.)

There are methods of generating a cryptographic signature for a document which proves its origin. (FOF ¶ 311.) Prof. Appel testified that although digital signatures exist, and Sequoia's marketing literature claims that the Advantage 9.00H employs such technologies, there are, in fact, no digital signatures to ensure the authenticity of results cartridge data. (FOF ¶ 313.) Therefore, there is no way to verify the authenticity of vote total data on results cartridges or on the motherboard of the Advantage 9.00H DRE. (FOF ¶ 310.)

The Union County Clerk, Joanne Rajoppi, has encountered serious problems in the operation of the WinEDS system. (FOF ¶ 652.) This causes her to doubt the reliability of the Sequoia AVC

Advantage 9.00H DRE and the accuracy of the election totals it generates. (FOF ¶¶ 650,657.) In the November 2008 general election, Ms. Rajoppi discovered that the WinEDS computer lost the results from all 438 Union County ballot cartridges that election workers had tabulated the night before. The election results had been "zeroed out." (FOF ¶ 652.) She and her staff had personally entered results manually the previous night and could re-create the data. (FOF ¶ 655.) But she still does not understand how the results were erased by WinEDS. (FOF ¶ 654.)

2. The Sequoia Advantage WinEDS System is Unreliable Because a Bug in WinEDS Causes the Advantage 9.00H DRE to Fail to Report Candidate Vote Totals.

Ms. Rajoppi testified about a bug that caused Sequoia AVC Advantage 9.00H DREs to fail to report vote totals for Carlos Cedeño, a candidate for the Union County Board of Chosen Freeholders, despite the fact that he was on the ballot and received votes. (FOF ¶ 876.) Ms. Rajoppi initially thought that the reason for this was the diacritical tilde in the "ñ" letter in his name. (FOF ¶ 646.)

However, Sequoia's Mr. Smith testified that the real cause of this bug is that WinEDS randomly assigned candidate Cedeño the candidate number "999." (FOF ¶ 877.) Mr. Smith also testified that there is no way to know when WinEDS will randomly assign a candidate this number and thereby cause Sequoia AVC Advantage 9.00H DREs to fail to report their vote totals. (FOF ¶ 877.)

Shockingly, Mr. Smith testified that Sequoia has been aware of this bug for some time, but chose not to disclose it to the State. (FOF ¶ 878.) Only after this bug caused the Union County Sequoia AVC Advantage 9.00H DREs to report erroneous vote totals did Sequoia finally issue a product bulletin warning of this bug. (FOF ¶ 878.)

V. PLAINTIFFS HAVE PROVEN THAT THE SEQUOIA ADVANTAGE DREs AND THE WINEDS SYSTEM ARE INSECURE AND READILY ACCESSIBLE TO HACKERS.

A. DREs CAN BE HACKED AT POLLING PLACES AND WAREHOUSES BY INSIDERS, CONTRACT WORKERS, AND THE GENERAL PUBLIC

Professor Appel demonstrated how easy it is to replace a ROM chip to make the Sequoia 9.00H cheat in a manner that cannot be detected. (FOF ¶ 116.) Professor Wolf testified that it is easy to create but difficult to detect a fake Z80 chip that can make the Sequoia 9.00H DRE cheat in elections. (FOF ¶¶ 1218-1219.) Thus, effective physical security is of the utmost importance to protect the Defendants' DREs. But no such physical security exists.

The Court heard the testimony of three voting machine warehouse workers. That testimony revealed how easy it is for insiders, the general public, and third party contractors invited into the warehouse by county employees to gain access to the Defendants' DREs.

1. The General Public Can Easily Access DREs at Polling Places and Hack the DREs.

Plaintiffs presented uncontested testimony that DREs are left at polling places unattended for weeks before each election and weeks after every election. The general public can tamper with these unattended DREs and install undetectable vote-stealing software.

From 2004 to 2008, Princeton Professor Edward Felten took several photographs of himself in front of unattended DREs throughout Mercer County. He took the photographs because, as a computer scientist who has worked on and studied DREs, (FOF ¶¶ 437-438), and also as a concerned citizen, (27: 17-19), Professor Felten was worried about the security of completely unguarded DREs. (27: 18-21.)

In polling places he visited and photographed DREs, the Sequoia Advantage DREs were left unattended. (FOF ¶ 463.) There were no guards in any of the buildings to watch over the DREs

(FOF ¶ 449.) All the hallways were unlocked and accessible to the public. (FOF ¶ 440.) No security badge or key was needed to access any of the buildings housing the DREs, and there were no alarm systems in any of the buildings. (FOF ¶ 469.) Furthermore, Professor Felten testified that no one approached him or talked to him as he was observing and photographing the unattended DREs. (FOF ¶ 445.)

More disturbing is that, at several locations, there were prominent signs outside the buildings, directing the public to the location of the DREs. (FOF ¶ 461.) Professor Felten was able to follow these signs directly to the unattended DREs. (FOF ¶ 461.)

Other witnesses confirm Professor Felten's testimony. In Ocean County, DREs are delivered starting five days before each Election Day. (FOF ¶ 510.) They are all returned five days after each Election Day. (FOF ¶ 511.) No one signs for the DREs when they are dropped off at the polling locations. (FOF ¶ 509.) No one is at the polling sites to receive the DREs. (78:3-11.) No one guards the DREs when they are dropped off at the polling sites. (FOF ¶ 507.)

Similarly in Hudson County, Penza Moving Company, an independent contractor, is hired to deliver DREs to polling places before an election and retrieve them after an election. DREs are delivered one week before election day, (FOF ¶ 516), and picked up a week after election day. There is no transfer of custody document. (FOF ¶ 508.) Penza employees do notify the Hudson County workers supervisors to make her aware that they have delivered the DREs to their respective destinations. (FOF ¶ 508.)

Similarly, In Bergen County, the Sequoia Advantage DREs are transported to polling places between ten days and two weeks before each election. (FOF ¶ 533.) The DREs are then left at the polling places for up to two weeks after the election. (FOF ¶ 537.) Bergen County does not provide any security for the DREs during that entire time period. (FOF ¶ 538.)

2. Warehouses Storing DREs Are Insecure

DREs are stored in warehouses year round that have sub-par and ineffective security. A large sign sits on top of the warehouse stating "Bergen County Voting Machines." (FOF ¶ 517.) There are no evening or weekend security guards at the warehouse. (2/23 89:5-6.) The back door entrance to the building has a three digit code shared by all warehouse employees. (FOF ¶ 520.) The code for the back door entrance was last changed five years ago. (FOF ¶ 520.) Even though each warehouse employee has a different a four digit code for the burglar alarm, Mr. Mahoney's code has not changed since the alarm system was installed 12 years ago, and codes for other employees have not changed since they were hired. (FOF ¶ 520.)

There are eight mechanics employed in the warehouse. (FOF ¶ 523.) They all have unlimited access to the insides of the DREs, and need no authorization to work on the DREs. (FOF ¶ 523.)

Inside the warehouse, the Sequoia Advantage DREs are lined up alphabetically. (FOF ¶ 521.) On the top of each DRE there is a piece of paper which identifies which town and district they go to. (FOF ¶ 521.) In the normal course of business, the keys which lock the DREs stay in the DREs. (FOF ¶ 522.) So, if someone were to access the warehouse with the intent of hacking DREs, they would know exactly which ones are going where, and they would not even have to pick the locks of the DREs. Similarly, before an election, ballot definitions are downloaded from WinEDS. During that time, the backs of the DREs are left open with the DRE keys sitting on top. (FOF ¶ 528.) At this time, anyone in the warehouse would have easy access to the ROM and Z80 chips because warehouse workers have access to the DREs without needing permission.

Bergen County has often lost the keys to DREs during elections. (FOF ¶ 539.) When keys to the Sequoia Advantage DREs are lost, Mr. Mahoney waits until the next election, and if the keys have still not been found he will then replace the locks on the affected DREs. (FOF ¶ 539.) During this lag time, someone could access the DREs using the "missing" keys.

Similarly, Ms. Gentile testified that the warehouse holding Hudson County's Sequoia Advantage DREs is not county owned, but rather rented from a Long Island resident. (FOF ¶ 478.) There is another tenant on the first floor. (FOF ¶ 478.) Six hundred DREs are stored on the second and third floors of the warehouse. (FOF ¶ 478.) There are no security video cameras installed at the warehouse entrance. (FOF ¶ 480.) There is an alarm system with a 4 digit code and each employee has a separate code, but that code has never been changed. (FOF ¶ 481.) There are no overnight or weekend security guards at the warehouse when the county employees are not working. (FOF ¶ 482.)

Hudson County's Sequoia Advantage DREs come with two sets of keys which open them. (FOF ¶ 498.) Sets of the keys have been lost in the past. (FOF ¶ 500.) There is a duplicate set of keys kept at the warehouse inside a filing cabinet, which was always kept unlocked until Ms. Gentile was deposed for this trial and realized how insecure the keys. (FOF ¶ 501.) There are no written policies for the warehouse employees about locking and unlocking the DREs. (FOF ¶ 502.) Before Ms. Gentile began to lock up the keys to her DREs any visitor to the warehouse, or even an employee, could have easily copied one or all of the keys to the DREs and returned them without anyone noticing.

Before an election and before DREs are sent to polling places, pre-LAT testing is conducted. At this time, the back doors of all DREs are opened and worked on by Election Graphics, an independent contractor chosen by Sequoia. (FOF ¶ 493.) Any willing person could use this opportunity to hack the DREs.

3. "Insiders" Pose The Greatest Risk to Tampering With the State's Election Equipment.

Dr. Shamos testified that "the principle threat that we worry about is what can insiders do." (FOF ¶ 1018.) According to Dr. Shamos, the insider threat is a legitimate security vulnerability. (FOF ¶ 950.) Dr. Shamos testified that "[a]n insider is someone who has unchallenged authorized access to a system and uses that access in an unauthorized fashion." (FOF ¶ 950.) "Insider threats occur when people who have authorized access to voting equipment do unauthorized things to the voting equipment, but normally they don't have to defeat regular security measures." (FOF ¶ 1018.) For example, "[i]f there's a lock, they have the key. If there's a password, they know the password." For an insider, "it's not difficult" to substitute ROMs. (FOF ¶ 1018.)

Insiders "who regularly replace chips because they're authorized to do so" would be able to conduct a switch. (FOF ¶ 957.) Furthermore, it is possible they could substitute ROMs even "if they weren't authorized to do so." (FOF ¶ 950.) "[T]he guy in the warehouse can do whatever, if he has authorized access to open the machine, then, you know, he could replace the entire innards of the machine if he wanted to." (FOF ¶ 950.) The vote totals could be manipulated by using their own personal computer. (FOF ¶ 956.) However, supervisors in multiple counties testified that little security exists in the warehouses and that background checks were rarely, if ever, conducted.

Additionally, the results cartridge can be corrupted by an insider who transports the cartridge. (Shamos 3/24, 165:9-10.) One can "prevent those insiders from doing things with physical interlock." (Shamos 3/24, 165:9-10.) Even transporters that do not have authorized access could open these locks, be unobserved, and corrupt the cartridge. (Shamos 3/24, 165:9-10.)

Additionally, employees who operate Win-EDS and set up ballot programming could "[c]ause great concern about inconsistencies in vote totals" and could cause through the audio daughterboard, cause the DREs to no function on Election Day. (FOF ¶ 965.) All voting machines have a "mechanism by which authorized service personnel can upgrade the firmware in the machine." (Shamos 3/25, 27:13-23.) Fraudulent firmware can be "surreptitiously introduced [by insiders] into the devices that the authorized technicians are using." (Shamos 3/25, 27:13-23.) Indeed, technicians may not even know they are installing malware into a voting machine. This would be difficult to detect. (Shamos 3/25, 27:13-23.)

Defendants have ignored the advice of their expert witness. A very basic and preliminary way to prevent "insider" jobs is through well-designed employee schedules and protocols "[b]ecause co-workers are going to know that you're doing something that is not on the regular schedule." (Shamos 3/23, 118:21-25.) At a bare minimum, Dr. Shamos recommends "storing the machines behind locked doors" or "storing them in warehouses where persons unknown would be immediately recognized as outsiders, or having 24-hour video monitoring in warehouses." (Shamos 115:15-25.)

4. DREs Can Be Hacked By Third Party Contractors.

New Jersey counties employ non-county employees and third party contractors to perform vital functions on DREs, including testing and updating the voting equipment. Most of the time, this is done with little to no supervision by county employees. Furthermore, no background checks are conducted on those hired to do this very important work. The unfettered access to DREs of third parties and non-county workers fits within Dr. Shamos' definition of an insider.

In Bergen and Hudson Counties, outside vendors are used to transfer the Sequoia Advantage DREs from warehouses to polling locations before elections, and from polling places to warehouses after elections. Those outside vendors are not accompanied by any county employees. There is ample opportunity for these outside contractors to tamper with voting machines. The contractors ride in the back of moving trucks with the DREs. Additionally, there is no transfer of custody papers between the county, the vendor, and the polling locations. The warehouse workers do not communicate with anyone at the polling locations to ensure that the DREs were delivered.

Furthermore, Win-EDS software, the AVC Advantage's vote tabulation equipment, is routinely handled by third parties. When the Win-EDS software on the Bergen County Sequoia Advantage DREs was upgraded, it was done by an independent outside vendor, Election Graphics, which was hired by Sequoia. Bergen County gave the vendor full, unsupervised access to Bergen County's DREs. (FOF ¶ 530.) The process of upgrading the software took between three and four weeks. (FOF ¶ 536.)

Similarly, for every election in Bergen County, ballot definitions are uploaded to Win-EDS computers by Sequoia, from a jump drive, a month before every election. This information is loaded one month before each election. (FOF ¶ 525.) The jump drive is never checked for corruption or viruses before it is put into the county's laptops. (FOF ¶ 526.) Neither Mr. Mahoney nor any other Bergen County employee has ever performed any tests to determine if the laptops have become corrupted. (FOF ¶ 525.) The ballot definition is then loaded on to the results cartridges, which are placed in the DREs. (FOF ¶ 525.) When this is happening, the backs of the DREs are open, and the keys are on top of the DREs. (FOF ¶ 528.) Anyone in the warehouse can easily access the insides of the DREs at this time.

Similarly, in Hudson County, pre-LAT testing is not conducted in-house. Election Graphics conducts pre-LAT tests before each election. (FOF ¶ 493.) The Division of Elections employees do not directly supervise Election Graphics. (FOF ¶ 494.) During the pre-LAT procedure, the back doors of all the DREs are left open. (FOF ¶ 484.) The pre-LAT process takes approximately two full days every time there is an election. (FOF ¶ 493.) During this time, the ROM and Z80 chips are accessible to all and can be manipulated.

As discussed above, third-party vendors and non-county employees are regularly hired to handle the Sequoia DREs and equipment. However, neither Ms. Gentile nor Mr. Mahoney could recall or confirm whether those handling DRE equipment had undergone a simple background check. Thus, the Defendants know nothing about who is handling their sensitive and inherently insecure voting equipment. Employing third parties to perform vital election functions unsupervised, combined with the fact that no one undergoes background checks is a serious security breach.

5. New Jersey Has No Protections in Place For Its Voting Machines.

Robert Giles, the Director of the New Jersey Division of Elections, testified that there are no uniform state-wide procedures or policies for the storage, maintenance, service or transport of Sequoia Advantage DREs from his office. (FOF ¶¶ 713-719.) Listed below are some key examples:

- There is no uniform state-wide policy concerning how DREs should be stored in county warehouses. (FOF ¶ 713.)
- There is no statewide policy for how keys for the DREs should be stored in each county. (FOF ¶ 714.)
- There is no uniform procedure for the pre-LAT examinations (154:3-6.) There is also no statewide recommendation for how many test votes should be cast during the pre-LAT examinations. (FOF ¶ 717.)
- There is no uniform state-wide procedure for transporting the DREs to and from the polling sites. (FOF ¶ 715.)
- There is no uniform state-wide policy for conducting security checks on the employees of private moving companies who transport the DREs from the warehouses to the polling sites. (FOF ¶ 716.)
- There is no uniform state-wide policy for the storage of cartridges used by the AVC Advantage DREs. (FOF ¶ 719.)
- There is no state directive as to how many votes should be cast during a pre-LAT test. (FOF ¶ 717.)

Plaintiffs' security expert, Dr. Roger Johnston, testified that New Jersey's overall lack of any security culture leaves its DREs exposed to tampering. (FOF ¶ 1089.) He was particularly disturbed by Mr. Giles and his "lack of a systematic approach to security." (FOF ¶ 1090.) According to Dr.

Johnston the Defendants' DREs are vulnerable in part because "it's clear that there is no plan or uniform policy or strategy for securing the voting machines either during storage, when transporting them, when locking them up, when leaving them in voting locales prior to the election." (FOF ¶ 1093.)

B. DREs CAN BE PURCHASED FROM THE INTERNET.

The general public is able to obtain DREs, including the Sequoia AVC Advantage, on which to practice stealing an election. Professor Appel testified that DREs are readily available to any member of the public freely intact on auction sites for very low prices. (FOF ¶ 130.) Professor Appel was able to acquire five Sequoia AVC Advantage version 5 DREs on the GovDeals.com auction site, on which federal, state, and local government agencies auction used or surplus equipment to the public. (FOF ¶ 130.) He paid a total of only $82 for all of them ($16.40 each). (FOF ¶ 130.) Professor Appel did not have to show any credentials before purchasing these DREs, nor did he have to reveal his motive for buying the DREs. (Id.)

The DREs Professor Appel purchased online were similar enough to the AVC Advantage 9.00H that it greatly assisted him in creating his vote stealing program. (FOF ¶ 130.) Professor Appel testified that an upgrade in firmware from an older version of a DRE obtained on the Internet to a newer DRE would not require a hacker to create a vote stealing software from scratch. (FOF ¶ 131.) The reverse engineering process could be started on an older version of the AVC Advantage firmware and would just need to be finished using information obtained from a DRE that is actually in use. (Id.)

C. ONCE AN ATTACKER GAINS ACCESS TO THE ROM CHIP, HE CAN REVERSE ENGINEER IT TO CREATE VOTE-STEALING SOFTWARE.

Once an attacker gains access to the motherboard and removes the ROM chip, he could acquire the source code from a Sequoia DRE's firmware by reverse engineering the ROM chips.

(FOF ¶ 131.) Defendants' expert, Dr. Shamos, agrees with Professor Appel that an undetectable vote-stealing program can be created by someone with ordinary computer training. (FOF ¶ 439.)

Reverse engineering is a common practice in computer science, (FOF ¶ 31), and would work just as well as the original source code would for creating fraudulent firmware. (FOF ¶ 132.) Reverse engineering the Sequoia DRE's firmware requires removing a ROM chip from the DRE. (FOF ¶ 135.) The legitimate ROM chip could be read with an inexpensive, commonly available ROM reader/programmer which cost only $149. (FOF ¶ 135.)

Thereafter, the legitimate ROM chip can be returned to the motherboard. The attacker can reverse engineer the source code at his leisure, away from the point of attack. (FOF ¶¶ 955-956.) Defendants' expert, Dr. Shamos, testified that ROM chips can be reverse engineered from the comforts of home to create vote-stealing programs. (FOF ¶ 956.)

Reverse engineering the ROM chip is a straightforward task which can be accomplished in several weeks, (FOF ¶ 132), with only a moderate level of computer knowledge. (FOF ¶ 132.) Professor Appel testified that a person with a Bachelor's degree or equivalent experience in computer science, (FOF ¶ 132), could reverse engineer a ROM chip to determine its source code. (FOF ¶ 132.)

D. WINEDS IS INSECURE AND CAN BE MANIPULATED TO CHANGE ELECTION RESULTS.

1. Vote-stealing Viruses From the Internet Can Infect Computers Running the WinEDS Election Tabulation Software and Can Propagate Through County Computers and Networks Used for Vote Tabulation.

WinEDS is an "election management system." (Smith 106:9-13.) Sequoia manufactures and sells WinEDS to work in conjunction with their AVC Advantage DREs. (FOF ¶ 574.) The WinEDS application serves a very prominent role in the election process: (1) before an election, WinEDS is used to prepare ballot definitions for Sequoia's DREs in conjunction with the Results Cartridge and Audio Ballot Cartridge, and (2) after an election, it is used to culminate the results from those same DREs. (FOF ¶ 389.) The application runs on ordinary, commercially available personal computers. (FOF ¶ 575.)

After examining the Union County laptop computer that ran the WinEDS program on Super Tuesday, Professor Appel concluded that it was "regularly and repeatedly connected to the Internet over a long period of time." (FOF ¶¶ 212-214.) He discovered "thousands" of saved files in the "Temporary Internet Files" folder stored on the Union County laptop. (Appel 1/29, 63:15.) Typically, when navigating the Internet with a commercial web browser like Internet Explorer, the browser will place Internet files into a folder stamped with a date. (Appel 1/29, 63:15, 63:19-24.) Thus, "Temporary Internet Files" placed into their respective folder create a record or log of Internet activity. (Appel 1/29, 63:13-18.)

Professor Appel examined these files and concluded that Internet Explorer was used numerous times on Union County's WinEDS computer to browse the Internet, download software, and even access a bank account on the day of the 2008 Presidential Primary election. (Appel 1/29, 65:12-18.) The dates culled from the files spanned a period of years that included "periods immediately before and after the February 2008 election." (Appel 1/29, 65:12-18.) This includes "the days leading up to and including the primary election of February 5, 2008." (Appel 1/29, 63:13-18.)

During this period, Internet files, maintained by Internet Explorer, revealed a "large number of websites visited for mail, shopping, personal banking, streaming music, pictures, and checking news and sports results." (Appel 1/29, 65:3-7.) The great majority of web browsing had little to do with Union County as only a small amount were related to Union County's official website, UCNJ.org. (Appel 1/29, 65:7-9.)

Professor Appel testified that each of the visits to these websites made the laptop computer susceptible to the ill effects of malware and malicious software. (Appel 1/29, 65:22-24, 66:1-8.) Malicious websites can exploit vulnerabilities in the operating system and have the potential to "insert viruses into the personal computer that's used to visit those websites." (Appel 1/29, 65:22-24, 66:1-8.) Furthermore, accessing the Internet allows a scenario where "outsiders can interfere with preparation of the ballots, can modify the results as they are added up, and change the data stored in the database." (Appel Report 23.1.) Therefore, as a rule, security-sensitive computers should not be used for casual web browsing. (Appel Report 23.4.)

Casual web browsing is highly problematic because "untrustworthy web sites can cause spyware and viruses to be downloaded onto the computer." (Appel Report 23.1.) "Each visit" to a website typically triggers "a host of downloaded images and tracking information from advertising sites, like Double Click, Dakota, [sic] Advertising.com." (Appel 1/29 65:9-12.) Thus, by accessing Internet, users unknowingly leave the computer "severely vulnerable" to malicious software. (Appel Report 23.4.)

The consequence of viral propagation via WinEDS can steal votes in multiple ways. First, before an election, a virus could "cause WinEDS to write fraudulent ballot definitions into (large-format) results cartridges." (Appel Report § 22.9, at 65.) Fraudulent ballot definitions could be designed that would miscount votes, such as by counting two votes for a candidate with a single button press from a voter. (Appel Report, § 43.1, at 94-95.) After an election, a virus could "cause WinEDS to fraudulently miscount votes, when it accumulates the results from different precincts," casting the results of the election into doubt if they differed from the results on the results report printouts. (Appel Report § 22.9, at 65.)

Secondly, viral propagation could reach the daughterboard of the AVC advantage via the Audio Ballot Cartridge or through a corrupted network connected to the Internet. Fraudulent firmware installed on the daughterboard can steal votes and disenfranchise voters in a number of ways. The most significant way is that it can change the votes of those voters who vote by audio, that is, blind voters or any voters who request to vote using the audio kit. (Appel Test., 1/29 Trial Tr. at 74:8-16.) The fraudulent firmware can change those votes before they are sent to the motherboard for tabulation. (Id.) Thus, disabled voters are more at risk from vote-stealing fraudulent firmware in the audio kit. (Appel Test., 1/28 Trial Tr. at § 24.4, at 69.7)

In addition to the threat to disabled voters, the vulnerability of the daughterboard to attacks can also impact the votes of non-disabled voters. (Appel Report, § 24.5, at 69.) Viral infection of the daughterboard can disable the motherboard when the computer is first turned on, thereby selectively disabling DREs in precincts selected by the attacker. (Appel Report, § 24.2, at 69.) The means the daughterboard uses to disable the motherboard is called a "buffer overrun" attack which disables the machine. An attacker might disable voting machines in selected precincts because they include a preponderance of voters of the party the attacker wants to lose. (Appel Test., 2/4 Trial Tr. at 21:12-22; Appel Report, § 24.5, at 69.) As Sequoia DREs fail, long lines would form, delaying voters from casting their votes. (Id.)

a. AmpX Was Downloaded from the Internet Causing Severe Vulnerabilities.

In addition to general web browsing, Professor Appel found America Online AmpX Music Streaming Service installed on the Union County laptop computer. (Appel 1/29, 67:7-9.) This service allows someone to listen to online music. (Appel 1/29, 67:7-9.) A computer security company, Symantec, has described AmpX as having a "high" severity vulnerability. (Appel Report 23.5.) An attacker exploiting the AmpX security vulnerability would produce a malicious music stream. (Appel Report 23.5.) The stream would then install a virus on the WinEDS computer. (Appel Report 23.5.) The attacker would have access to the WinEDS computer and would be able to modify the WinEDS vote database or the WinEDS vote-counting program. (Appel Report 23.5.)

The AmpX service was "regularly" used on the Union County laptop computer allowing Internet hackers to take over the Union County's WinEDS computer. (Appel 1/29, 67:4-7.) Thus, the possibility exists for an "attacker anywhere on the Internet" to interfere and subvert the main functions of WinEDS." (Appel 1/29, 69:15-24.)

b. Should a WinEDS Computer Be Connected to the Internet, Microsoft Windows Has Well-Known Security Vulnerabilities That Can Be Exploited to Corrupt WinEDS.

The WinEDS laptop computer examined by Professor Appel was equipped with the Microsoft Windows XP operating system and standard software such as Internet Explorer 7.0, Microsoft Office, and Windows Media Player. (Appel 1/27 176:20, Appel Report 22.2-3.) Notably, Microsoft Windows and Internet Explorer contain security vulnerabilities continually discovered in the operating system on a month-to-month basis. (Appel 1/29, 65:22-25, 66:1-3, Appel Report 23.3.)

Although Microsoft tries to "patch" these vulnerabilities, users of the operating system should expect vulnerabilities at "any given time." (Appel 1/29, 65:22-25, 66:1-3.) These vulnerabilities expose the computer, the WinEDS election management program, and its data to an Internet attack. (Appel Report 23.1.) Thus, Sequoia's voting machines are heavily reliant on Microsoft Corporation because Sequoia has little control over Windows or other Microsoft applications. (Shamos 3/23, 165:15-17.) Consequently, WinEDS computers are susceptible to all Internet attacks successfully used "every day" to infiltrate ordinary Windows computers. (Appel report 28.2.) This includes Internet viruses, websites containing spyware, port scanning, and e-mail phishing. (Appel report 28.2.)

Microsoft Windows, communicates "with the outside world" with a large variety of "services" and "protocols" that are employed to connect with the Internet. (Appel Report 23.6.) Each of these services and protocols are communicative devices that "constitute[] a vector" in which attackers anywhere on the Internet can insert malicious software onto a computer used to browse the Internet. (Appel Report 23.6.) Therefore, in order to preserve the integrity of computers handling information requiring protection, the services of the computer's operating system should be configured to "minimize the number of attack vectors." (Appel Report 23.7.)

"One common vector that Internet scammers use to infect PCs with malware is by e-mail attacks." (Appel Report 23.8.) Opening a "bogus email attachment" can cause a malicious attack. (Appel Report 23.8.) Thus, computers used to access email and to employ WinEDS causes a large security concern. (Appel Report 23.8.)

Professor Appel found that the Union County laptop did not minimize these vectors because it had a large number of services automatically enabled. (Appel Report 23.7.) These services include SQL Server, Universal Plug and Play, Net Logon, and Remote Registry. (Appel Report 23.7.) Additionally, the Window firewall was disabled, but a port scan of the machine revealed several open Transmission Control Protocol (TCP) ports and a dozen User Datagram Protocol (UDP) ports. (Appel Report 23.7.) All of these programs and open ports constitute potential vectors that can be opportunities to attack Windows or WinEDS. (Appel Report 23.7.)

These security vulnerabilities are highly problematic because the WinEDS application itself is insecure. (Appel Report 27.1.)

c. WinEDS Equipped Computers Are Connected to the Internet in Other Counties.

The Dell laptop computer from Union County Dr. Appel examined is typical of other

WinEDS laptops used throughout New Jersey. Testimony by election officials from Union, Mercer, Hudson, Ocean and Bergen counties reveals that WinEDS computers have Internet access and are used to connect to the Internet. Moreover, Mr. Giles, the Director of the New Jersey Division of Elections, admitted that his office has not issued a directive prohibiting laptops or computers used to transmit election information from being connected to the Internet." (Giles 3/3 110:23-24, 157:17-25.) The Defendants presented no witnesses whatsoever who in any way rebutted testimony that counties connect their voting systems to the Internet. This is problematic because any WinEDS computer used to connect to the Internet presents severe security vulnerabilities. (Appel Report 23.1.)

The Voting Machine Certificate Committee knew the WinEDS System could be connected to the Internet but still recommended that it be certified despite these serious vulnerabilities. As discussed above, the Committee did not consult with any computer scientists or security experts to determine the effects of an Internet connection to the overall reliability and security of the voting systems. (Mahoney 2/24, 31:9-16.)

d. Any Computer Connected to Both the Internet and Internal Network Can Corrupt the Whole Network.

If any computer on a network is connected to the Internet, a viral infection can propagate to a WinEDS computer also sitting on that network. Networks with Internet access allow viral propagation because "[a] computer virus is a program that can copy itself from one computer to another, either through computer networks or through removable media such as cartridges." (Appel Report 20.2.) This can compromise the "the integrity of the ballot preparation process and the integrity of the election tabulation process are compromised." (Appel 1/29, 70:15-17.)

WinEDS is a database arranged as a "client server system" and for the "proper function of WinEDS in a county, the computers generally need to be connected to each other through a network." (Appel 1/29 71:19-23, 72:1-6.) A client server system has two parts: (1) a database server and (2) "client computers" that connect to the server. Here, a "database server contain[s] ballot and election tabulation data." The "client computers" running WinEDS interact with the Results Cartridges and Audio Ballot Cartridges to communicate with the DRE and gather the election data.

In order to process all the election results in a county, the client computers need to transmit data to the "server machine." This can happen through a local network and "[g]enerally, the different WinEDS computers in a county are connected to each other by a network." (Appel 1/29, 70:4-5.) Either laptops, like Union County's WinEDS computer, or desktop computers "can connect to it on a local network at the Board of Elections."

Any one computer connected to the Internet on that network can facilitate viral propagation over the county's entire network. (Appel 1/29 70:4-10.) Accordingly, if a WinEDS computer connected to the network can succumb to viral infection without itself actually being connected to the Internet. (Appel 1/29 70:4-10.) "If that network is connected to the Internet, then the infection from the Internet of even one machine on that network can propagate to all of the other WinEDS machines in that county's network." (Appel 1/29 70:7-10.)

Viral propagation works both ways as well. If a virus resides on a WinEDS computer and that computer is connected to a network, the virus "can copy itself onto other WinEDS computers on the same network." (Appel Report 20.6.) Having any WinEDS computer accessing the Internet allows for an Internet virus to propagate through "through County or State internal networks, to other WinEDS computers." (Appel Report 22.9.)

e. Should Any WinEDS Computers Become Corrupted, the Integrity of the Results Cartridge Becomes Suspect.

Once a virus propagates onto the WinEDS computer, the virus can adversely affect data residing on the Results Cartridge. (Appel Report 22.9.) A virus could "cause WinEDS to write fraudulent ballot definitions into (large-format) Results Cartridges." (Appel Report 22.9.) Furthermore, a virus could "cause WinEDS to fraudulently miscount votes, when it accumulates the results from different precincts." (Appel Report 22.9.) In other words, "malicious software can change ballot definitions (before elections) and change vote data (after elections)." (Appel Report 23.17.)

The Results Cartridge is an integral piece of the DRE's setup and is the primary vehicle to transmit information from WinEDS, a database coordinating all election data, to the AVC advantage and vice versa. The Results Cartridge has two broad responsibilities in the election: (1) the "cartridge is used to convey the ballot definition to the voting machine before the election" and (2) the cartridge is used to "convey the results back to the WinEDS after the election." (Appel 1/28, 6:14-19.) The cartridge is about the size of a VHS tape and typically has 96 kilobytes of storage capacity. (Appel 1/28, 6:23-25, Appel Report 2.5.) Each cartridge is reusable and there is no protection against reading and writing data in the cartridge and a corrupted WinEDS computer can change election data. (Appel Report 40.2.)

The WinEDS application is used to coordinate all of the DREs via the many Results Cartridges. Accordingly, the portable Results Cartridge must transmit and receive data and instructions from the WinEDS computer. (Appel 1/27 177:3-12.) To do so, the Results Cartridge is linked to a WinEDS computer via a "cartridge reader writer." (Appel 1/27 177:3-12.) The "cartridge reader writer" connects to the WinEDS computer by connecting a USB cable drawn from the reader writer to the computer's USB port. (Appel 1/27 177:3-12.) The "cartridge reader writer" has the ability to read election data as well as write data onto a Results Cartridge when attached to a WinEDS computer. (Appel 1/27 177:3-12.) Thus, if the WinEDS computer is corrupted, the information on the Results Cartridge can be corrupted before and after an election.

Before an election begins, election workers use WinEDS to write ballot definitions into Results Cartridges. A ballot definition informs the AVC Advantage of the candidate's names and the names of the contests. (Appel 1/27, 173:3-7.) Additionally, the ballot definition informs the DRE of which candidates are running in which contests by coordinating "the buttons on the full face ballot" to correspond with the respective candidates. (Appel 1/27, 173:3-7.)

In order to write the ballot definition, the Results Cartridge is placed into the "reader writer" that is linked to the WinEDS Computer and WinEDS runs tests, "clears what's there previously[,..] checks its [b]attery[,] and the read writability." (Clayton 2/26, 195:1-7.) Then WinEDS programs the Results Cartridge for a particular DRE, by writing the ballot definition into the Results Cartridge and prepared data "about the layout of the ballot" is copied onto the Results Cartridge for each voting machine. (Appel 127, 179:3-6.) Should any incorrect information find its way onto the DRE via the Results Cartridge, the DRE's record of votes cast would not correspond with the voter's intent.

After the Election and after the polls close, the AVC Advantage communicates vote totals to election officials by first, printing a paper Results Report printout and secondly, writing the totals and a ballot images onto the Results Cartridge. (Appel Report 2.5.) Stored on the motherboard of the AVC Advantage is another copy of the ballot images. (Appel 1/28, 112:8-9.) Again, in order to read the ballot images and the vote totals, the Results Cartridge is connected to a WinEDS computer via the "reader writer." (Appel Report 2.5.) After the Results Cartridge is inserted, the WinEDS software "extract[s] the election results and cumulate[s] the results from all the precincts." (Appel Report 20.5.) Thus, if a computer is connected to the Internet and infects WinEDS, the vote data on the Results Cartridge can be infected or lost because WinEDS has the ability to read and write onto the Results Cartridge.

f. Viral Propagation Can Infect the Daughterboard of the AVC Advantage Making The Votes of Blind Voters Particularly Susceptible to Vote-Stealing Internet Viruses.

There are three ways that an infected WinEDS computer can corrupt the daughterboard of the Sequoia AVC Advantage DRE: (1) a virus can propagate from the audio ballot cartridge to WinEDS, (2) a virus can propagate from WinEDS to the audio ballot cartridge, and (3) a virus can propagate from WinEDS to other WinEDS computers on the same network (FOF ¶ 266.) Viral infection of the daughterboard can disable the motherboard when the computer is first turned on, thereby selectively disabling DREs in precincts selected by the attacker (FOF ¶ 261.)

A virus already affecting or resting on a WinEDS computer can infect the audio ballot cartridge when connected to the computer. An audio ballot cartridge connects to a personal computer through a standard Personal Computer Memory Card International Association ("PCMCIA") port on the laptop computer by using a standard PCMCIA extender card. (Appel Report, 22.4; FOF ¶ 254; Pl. Ex. 11.) Should the WinEDS computer be infected or become infected by an audio ballot cartridge, every audio ballot cartridge it comes into contact can be infected and be used, even unknowingly, to infect its companion DRE. (Appel Report, 22.9.)

Fraudulent firmware installed on the daughterboard can steal votes and disenfranchise voters in a number of ways. (FOF ¶¶ 260, 265.) The most significant way is that it can change the votes of those voters who vote by audio, that is, blind voters or any voters who request to vote using the audio kit. (FOF ¶ 260.) The fraudulent firmware can change those votes before they are sent to the motherboard for tabulation. Thus, vote-stealing fraudulent firmware in the audio kit can severely effect the votes of the disabled. (Id.)

Furthermore, the general voting public can be affected if the audio ballot cartridge disables the motherboard of the DRE with a "buffer overrun" attack. A "buffer overrun" occurs when a user or a program returns invalid input in response to a request by a computer program, generally a longer string of data than the requesting program wants. The effects of the buffer overruns happen when the DRE is powered on. Its motherboard will request input from the daughterboard, which will then send a malicious message, causing it to reboot. (Id.) This cycle will repeat indefinitely and completely disable the DRE. (Id.) An attacker could disable machines in specific areas that have a preponderance of voters the attacker wants to lose.

g. Defendants' Witnesses Agree with Professor Appel that Any Connection to the Internet Raises Serious Security Concerns.

Defendants' expert witnesses agree that availability and use of the Internet on a WinEDS computer raises security concerns regardless of whether the computer has actually been hacked. (Shamos 3/23 154:6-12, 13-15.) The Court recognized this when she stated, "We've got a lot of witnesses who testified to [the internet connection being problematic]. There's nobody who says [the Advantage] should be [connected], and I'll stipulate to that." (Fleming 4/1 46:17-25.)

Dr. Shamos testified that computers connected once to the Internet or computers with a permanent connection are "a bad and terrible thing." (Shamos 3/23 153:22-25, 154:1-3.) Furthermore, Dr. Shamos testified that a WinEDS computer used to browse the Internet is "never permit[ted] in the states where [he does voting machine] certifications." (Shamos 3/23 154:1-2.) In his report, he states, "I agree that voting machines and computers on which election management software is installed should never in their lives be connected to the Internet." (Shamos Report ¶ 105.) Speaking about WinEDS, he stated, "from day one when it's delivered until it dies, you never connect it to the Internet." (Shamos 3/23 154:16-17, 159:16-17.) If the computer is connected at any time during its life and "not just, let's disconnect it now and then run the election," the computer can "pick up" a virus during if one connects to the Internet. (Shamos 3/23 154:13-19.) "Anybody who is connected to the Internet can pick up viruses." (Shamos 3/23 154:20-21.)

Dr. Shamos also recognized the security vulnerabilities of email. Email allows for a network and its computers to be susceptible to outside manipulation. (Shamos 3/23 157: 10-20.)

Sequoia's Edwin Smith also agrees with Professor Appel that "connection of WinEDS computers to the Internet constitutes a significant security threat." (Smith 3/19 32:19-22.) He testified that "election-related computers never be attached to the Internet but instead be kept on an isolated network." (Smith 3/18, 118:5-8.) In fact, he claims, "[t]he first thing you do is never hook them up to the Internet." (Smith 3/19, 110:20-21.) This is because when "connecting a voting system to the Internet, . . . the integrity of the system can be compromised." (Smith 3/19, 85:4-7.) After becoming aware that Union County's computer was connected to the Internet, Smith recommended that Union County "should be sanctioned for [allowing] that." (Smith 3/19, 111:4-6.) Given Mr. Smith's acknowledgement that Internet connections pose serious security threats, it is irresponsible that Sequoia continues to manufacture and sell voting systems with Internet connectivity. Moreover, it is also irresponsible that Sequoia never discussed these Internet-related insecurities when it presented the WinEdS system to the voting machine Certification Committee in 2006, (see Exh. P-50.)

VI. "SECURITY MEASURES" CONTEMPLATED BY THE STATE FOR USE ON DREs AND WINEDS DO NOT PROTECT THEM FROM TAMPERING

A. THE COURT SHOULD GIVE LITTLE WEIGHT TO SECURITY SEALS AND MEASURES PROPOSED FOR USE BY THE STATE.

The Defendants have proposed a series of security measures throughout the course of the trial which they withdrew as quickly as they introduced. Some of these security measures do not even exist. They are no more than aspirations.

This Court should give little weight to testimony about those security measures. The seals proposed by the Defendants are not part of the AVC Advantage DRE. If admitted evidence "suffer[s] shortcomings when measured by the strict rules of evidential relevance and competence," the trier of fact is responsible for "separating the wheat from the chaff," State v. Davis, 96 N.J. 611, 623 (1984). The Court is therefore "free to give that testimony as much or as little weight as [the court] deem[s] appropriate." Bolshakov v. Borok, No. DC-1487-07, 2009 WL 425934, *1 (App. Div. Feb. 20, 2009); see City of Atlantic City v. Ace Gaming, LLC, 23 N.J. Tax 70, 78 (2006) (noting that court gave testimony found to be of "minimal relevance" little weight).

1. Security Measures Not Presently Used on the AVC Advantage Are of Little Weight.

Security measures that are not currently in use on the AVC Advantage DRE are not probative of the DREs' security, and thus are not useful or probative in any way in determining liability. For example, in Saldana v. Michael Weiniq Inc., a photograph of an allegedly faulty molding machine was held to have no probative value because it contained an image of a warning sticker which was not an accurate reproduction of what the machine in question looked like at the time of the accident. 337 N.J. Super. 35, 47 (App. Div. 2001) (ruling a photograph should have been cropped to eliminate warning sticker and introduced on limited basis to show point of operation.) Similarly, in State v. Allison, where prosecutors sought to determine the cause of a fire, evidence of drug paraphernalia found two months prior to a fire, in a location other than where the fire originated, was not probative of cause and was properly excluded. 208 N.J. Super. 9, 17 (App. Div. 1985).

Since November 2008, the Defendants have introduced no less than thirteen different seals it has considered installing in the AVC Advantage. (FOF ¶ 1075.) Those proposed security measures include the: (1) plastic strap seal; (2) red adhesive tape with a New Jersey state seal; (3) wire cable lock seal; (4) large cup seal; (5) blue plastic strap seal; (6) revised blue plastic strap seal; (7) small Brooks MRS pressure-sensitive seal with ultraviolet markings; (8) large Brooks MRS2 pressure-sensitive seal; (9) Brooks padlock seal; (10) small cup seal; (11) small cup seal with Gorilla Glue; (12) large cup seal with Gorilla Glue; and (13) Brooks red adhesive tape seal. (FOF ¶ 1077.)

The Defendants summarily abandoned almost half of the above-mentioned seals within a month of proposing them, including the: (2) red adhesive tape with a New Jersey State seal; (3) wire cable lock seal; (4) large cup seal; (5) blue plastic strap seal; (10) small cup seal; and (12) large cup seal with Gorilla Glue.

In fact, the Defendants proposed and subsequently abandoned so many security measures that even the Defendants do not know which measures it intends this Court to consider when assessing the security of the AVC Advantage DRE. As Dr. Johnston testified at trial, "every time I started to look at a seal, a new seal would arrive and the old seal would no longer be of merit." (Johnston Test., 4/22 Trial Tr. at 15:19-23.) Further, illustrative of this point is an exchange which occurred during Dr. Johnston's testimony about the Defendants' plan to install a large cup seal.

Court: That's not being used, right?

Ms. Gore: No, it's not being used.

Ms. Venetis: Should I just stop?

Court: Yes, they aren't using it.

Ms. Venetis: Okay.

Court: I just want to make sure there's no problem later.

Ms. Gore: Big cup seal.

Mr. Giles:
(from the gallery) It could be. I don't want to rule anything out, in all fairness.

(Johnston Test., 4/21 Trial Tr. 167:24–168:7.) Indeed, on May 11, 2009, the last day of trial, the Defendants were still attempting to introduce new security measures; this time in the form of tape stamped with a serial number. (Giles Test., 5/11 Trial Tr. 68:21-71:9.) While Mr. Giles at first tried to argue that the security tape was the same tape the Defendants previously provided to Dr. Johnston, he eventually acknowledged that he was proposing using a never-before-seen security measure.

> Q: D-31. Were you told that's the exact same as the tape that Dr. Johnston was given.
>
> A: Yes. It's called KT Plus.
>
> . . . .
>
> Q. Well, that's a smaller serial number; is that correct?
>
> A: I would have to look at the other one, but it's a different size seal because it's not on the tape.
>
> Q: So it's not the exact same seal; is that correct?
>
> A: Correct.

(Id. at 74: 3-20.) This Court has already held that any previously undisclosed security measure "is of no relevance," (id. at 68:8-10), and that "the Court really cannot draw any conclusions as to whether or not that's going to make [the DRE] more secure or not." (Id. at 70:4-9.)

As such, the Defendants' ever-changing and purely speculative list of potential security measures is of little weight and lacks any probative value to the legal issue in question: the insecurity of DREs actually in operation in New Jersey. Like the sticker in Saldana and the drug paraphernalia in Allison, the Defendants' potential security measures are not probative of the security issues in this case because they are not actually part of the voting system being evaluated by the Court. The Defendants have not actually purchased any security measures; have not sent out any Requests for Proposal to vendors; and cannot say with certainty which security measures, if any, they will actually use in future elections. As Mr. Giles explained at trial:

> Q: So you don't know which security measures the State of New Jersey is planning on using in the future, isn't that correct?

A: Currently, we've headed in the direction of the high security padlock, the smaller cup seal and some type of tamper-evident tape at this point. But if a company comes with, with a product that might help secure the machine even more, that's something we will look at.

Q: So there are no requests for proposals out to supply the State of New Jersey with security measures, is that correct?

A: That's correct.

(Id. at 174:6-19.)

Additionally, as the Defendants have not developed any use protocols for these potential security measures, it is not even clear how the seals would be used if acquired. The following testimony by Dr. Johnston of Gorilla Glue demonstrates this point.

Q: Dr. Johnston, you mentioned earlier that you've learned that the State of New Jersey is contemplating the use of Gorilla Glue for placement in the cup seals: is that correct?

A: Yes.

Q: From a security perspective, what is the impact of placing Gorilla Glue in a cup seal?

A: Well, it represents a number of problems. We don't have, again, a full use protocol, and nor do we fully understand the gluing technique. . . . But because we don't have any of the actual use protocol, it's not clear exactly how this glue should be installed. . . . But without knowing the amount of glue that should be applied, without having the data on the type of applicator that should be used, it's very difficult to try to replicate what Mr. Giles had in mind if, indeed, he had something in mind.

(Johnston Test., 4/21 Trial Tr. 171:20-172:22.)

The Defendants have made clear that they have no definite plan concerning security measures they will use in the Sequoia AVC Advantage DREs in the future. The Defendants have not finalized a list of security measures; and in fact, until the last day of trial the Defendants were still proposing new security measures. The Defendants have taken little to no affirmative steps to acquire any of the multitude of security seals they have proposed to use. Accordingly, this Court should give little weight to any proposed security seal that is not presently installed on the AVC Advantage, including the thirteen proposed security seals that Dr. Johnston examined and defeated.

2. Security Measures Which Do Not Physically Exist and Are Purely Theoretical Should Be Given No Weight by the Court.

Two of the seals and security measures that the Defendants seek to have this Court consider (the ultraviolet tape, and the small cup seals with serial numbers) do not even exist. As this case concerns the security of the AVC Advantage DRE as it is currently in use in the State of New Jersey, theoretical and purely aspirational security measures that may never be produced, let alone installed in the AVC Advantage should be given absolutely no consideration.

In December 2008, the Defendants stated they would be adding a tape with an ultraviolet marking to the AVC Advantage DRE as a security measure. Now, seven months later, an example of the tape has yet to be produced. When asked specifically about the small Brooks MRS seal with an ultraviolet marking, Dr. Johnston testified that:

> Q: And have you seen any samples of this, of this logo?
>
> A: Well, I've seen an ultraviolet fluorescing logo on a piece of plastic with the implication, I guess that this one potential logo that could be applied to the tamper-indicating seal.
>
> Q: But have you seen an actual sample of what will be used in the voting machine?
>
> A: My understanding is that the seal does not exist in the form of an ultraviolet logo from the manufacturer.
>
> Q: I'm sorry, can you please repeat your answer because I didn't hear you.
>
> A: My understanding is that the manufacturer, Brooks, does not currently provide that seal with an ultraviolet logo, through it has discussed that would be an option.

(Johnston Test., 4/21 Trial Tr. 120:8-24.) It is irrelevant that Brooks has discussed that ultraviolet tape may be an option at some indeterminate time in the future. Only security measures that are actually installed on the AVC Advantage and have been examined by

Plaintiffs' experts should be given any weight by the Court.

Similarly, the small cup seals with serial numbers have never been provided to Plaintiffs and are not available to the Defendants. The small cup seals that Dr. Johnston was provided to examine did not have any serial numbers on them. (Id. at 147:21-148:15.) Further, American Casting and Manufacturing, the company that produces the cup seals, told Dr. Johnston that the company was both discontinuing the seals' production and will not place serial numbers on those seals. (Id. at 149:25-150:11.) The Defendants have not produced such a seal and did not introduce one at trial. When Mr. Giles was specifically asked if he had ever seen a cup seal with a serial number, he candidly admitted, "No, but we were preparing – [one]." (Id. at 71:18-72:2.)

Theoretical security measures that are only in the preparation stage, have never been completed, and which have not been examined by Plaintiffs' experts have no probative value and should not be considered at all by this Court in deciding the Defendants' liability or in fashioning a remedy.

The Defendants' security measures are speculative at best; and imaginary at worst. The Plaintiffs should not have to prove that a non-existent moving target is insecure. Liability is predicated upon the DREs as they exist in New Jersey today. Thus, it is the DREs that Professor Appel examined that Plaintiff should have to demonstrate violate Title 19 and the New Jersey Constitution.

B. THE STATE'S HAPHAZARD APPROACH TO PHYSICAL SECURITY DOES NOT PROTECT DREs.

The Court heard extensive testimony about the poor physical security of New Jersey's DREs from Plaintiffs' expert witness Dr. Roger Johnston, a Senior Systems Engineer at Argonne National Laboratories. (FOF ¶ 1061.) Ross Anderson, Professor of Security Research at Cambridge University, has written that "the most impressive physical security research team in the world is probably Roger Johnston's Vulnerability Assessment Team." (FOF ¶ 1068.)

The Defendants never called any witnesses with any expertise in physical security. (FOF ¶ 1072.) Thus, Dr. Johnston's testimony is the only testimony before the Court on the subject of physical security as it relates to New Jersey's DREs. (FOF ¶ 1072.) His conclusions — that New Jersey has no security culture, and that the Defendants' proposed secret measures can be defeated without detection — are uncontested. (FOF ¶ 1072.)

1. The State's Proposed Seals Cannot Provide Effective Security For The State's 11,000 DREs, Because New Jersey's Has No Security Culture.

Dr. Johnston testified that "one can't have good security no matter how good the hardware if one doesn't have a good security culture." (FOF ¶ 1073.) An organization with a healthy security culture, according to Dr. Johnston, builds security into everything it does, at every level: it engages in critical self-review; approaches security proactively; incorporates a desire to improve security into every level of the organization; and eagerly solicits input on security from all quarters, both internal and external. (FOF ¶ 1073.) It does not wait passively for security problems to be pointed out by an external agent, (FOF ¶ 1073) or respond in an ad hoc way to vulnerabilities by "slapping on" some third-party solution. (FOF ¶ 1073.) Indeed, as Dr. Johnston testified, a healthy security culture regards security not as a commodity for sale, but as an ongoing process integral to all operations. (FOF ¶ 1073.)

Dr. Johnston concluded that New Jersey suffers from an unhealthy security culture with regard to its DREs, making elections conducted on the DREs vulnerable to numerous attacks. (FOF ¶ 1074.)

2. An Example Of The State's Poor Security Culture Is That It Has Introduced Numerous Security Seals, Many After Trial Started, Without Crafting Any Use Protocols For Applying and Inspecting The Seals.

Perhaps no better indication of New Jersey's unhealthy security culture exists than its approach to security seals on the eve of trial and during trial. Dr. Johnston examined no fewer than thirteen seals since he became involved in this case in 2009. (FOF ¶ 1075.) All of the seals were introduced after the discovery phase had already ended. (FOF ¶ 1075.)

The Defendants did not consult any independent security experts before introducing security seals. (FOF ¶ 1076.) Additionally, the Defendants have changed seals in response to advice gleaned from Plaintiffs' expert testimony; a reactive, rather than a proactive, approach. (FOF ¶ 1076.) The Defendants' ad hoc measures leave the DREs open to multiple attacks. (FOF ¶ 1076.)

The Defendants began introducing its security seals in November 2008, two months before trial was to begin. (FOF ¶ 1077.) This was many months after Professor Appel demonstrated that the Sequoia Advantage 9.00H DRE could be hacked to steal votes in less than 7 minutes by replacing the DRE's legitimate ROM chip with a fraudulent one. (FOF ¶ 1077.) Since November 2008, New Jersey has introduced twelve new security seals:

1. Plastic Strap Seal---no evidence was provided by the State on how long these seals have been used. Of the two DREs given to Professor Appel to examine, only one had a Plastic Strap Seal installed.

November 13, 2008:[6]

2. Red Adhesive Tape with New Jersey State seal[7]
3. Wire Cable Lock Seal[8]

[6] Certification of Professor Andrew Appel, ¶ 5, Dec. 1, 2008, Docket No. MER-L-2691-04.

[7] The security markers in this seal are covered by the protective order, and will be discussed in a later section of this submission that will be redacted from the public version of this submission.

[8] The State has made multiple representations to the Court that this seal was no longer being contemplated for use.

4. Large Cup Seal

5. Blue Plastic Strap Seal

December, 2008

6. Blue Plastic Strap Seal

7. Small Brooks MRS2 Pressure-Sensitive Seal with Ultraviolet Markings[9]

(This seal does not exist)

8. Large Brooks MRS2 Pressure-Sensitive Seal

9. Brooks Padlock Seal

10. Small Cup "Seal"

(This "seal' does not exist with a unique serial number)

April 9, 2009

11. Small Cup "Seal" with Gorilla Glue

12. Large Cup Seal with Gorilla Glue

13. Brooks Red Adhesive Tape Seal

(FOF ¶ 1077.)

The Defendants' poorly planned and hasty introduction, withdrawal, and re-introduction of seals has not made the Defendants' DREs safer in any way. (FOF ¶ 1077.) Evidence of this is that Professor Appel, who is a not a burglar, defeated all of the seals proposed by the Defendants.

Dr. Johnston's opinion is that New Jersey, like other "organizations with poorly thought-through security pile[s] on multiple security features, devices, or layers in hopes that the complex interaction of all these layers will somehow automatically add up to good security." (FOF ¶ 1078.) He testified, further, that it takes at least several months per seal of intensive work and training to develop effective seal use protocols. (FOF ¶ 1078.)

3. The State Proposes To Cover Deep, Inherent Security Flaws By Using A Superficial "Band-Aid" Approach.

The sheer number of seals proposed by the Defendants demonstrate its lack of a coherent security policy for New Jersey's DREs. (FOF ¶ 1079.) New Jersey proposes to use six different seals in nine locations on its DREs. (FOF ¶ 1079.)

Dr. Johnston testified that in seventeen years at the forefront of his field, he has never seen so many seals used at once, including on top-secret nuclear safeguards and other high-level national-security applications. (FOF ¶ 1080.) The most seals he has ever seen in one application was three. (FOF ¶ 1080.)

This is because in order to have effective security systems, security professionals consciously minimize the complexity of their programs. (FOF ¶ 1081.) Each new seal added to a system multiplies the complexity of the use protocols necessary to ensure its effectiveness. (FOF ¶ 1081.) As Dr. Johnston testified, "with security, as with many things in life, simplicity is the best approach." (FOF ¶ 1081.) Complexity, on the other hand, both compounds the cost of a security program and introduces new vulnerabilities. (FOF ¶ 1081.)

Dr. Johnston concluded that the unprecedented complexity of New Jersey's seals will overwhelm seal inspectors, as they struggle to do a good job on every seal under a more and more minutely detailed rubric. (FOF ¶ 1082.)

4. New Jersey Has Not Established Protocols Governing The Use Of Its Proposed Seals, And Therefore Cannot Use Them Effectively.

Dr. Johnston testified that "a seal is . . . no better than its use protocol." (FOF ¶ 1083.) Without protocols, the proposed seals cannot fulfill their most basic security function. New Jersey currently has no protocols in place governing how it will use its proposed security seals. (FOF ¶

[9] The security markers in this seal are covered by the protective order, and will be discussed in a later section of this

1083.) Without rigorous protocols governing every aspect of their use, the proposed security seals will not provide effective security. (FOF ¶ 1083.) Seal use protocols should govern seals "from cradle to grave:" how they are chosen, procured, used, transported, installed, inspected, removed, disposed of, how training is done, who the personnel are, and so on. (FOF ¶ 1084.)

The reason for establishing use protocols is that tamper-indicating seals are only as effective as they are predictable. (FOF ¶ 1085.) Seal inspectors must know how a seal is supposed to look and behave in order to inspect it. (FOF ¶ 1085.) For seals to look and behave predictably, they must be installed, handled, and inspected in a consistent way. (FOF ¶ 1085.)

Dr. Johnston concluded that New Jersey's lack of any security protocols gravely compromises election security. (FOF ¶ 1086.) First, New Jersey has no protocol governing proposed seal installations. (FOF ¶ 1086.) Seals, according to Dr. Johnston, often suffer incidental damage, such as inadvertent scratches or dents, during installation. (FOF ¶ 1086.) No protocol exists in New Jersey either ensuring consistent installation techniques or directing personnel to take notice of incidental damage inflicted during installation. (FOF ¶ 1086.) A seal inspector confronted with a damaged seal, but with no way to discern whether the damage is evidence of tampering or merely incidental, has no sound basis to determine whether or not an attack has taken place. (FOF ¶ 1086.) As a result, election security suffers. (FOF ¶ 1086.)

New Jersey also has no protocols in place for inspecting seals. (FOF ¶ 1087.) Because the essential function of seals is to detect tampering, seals are only as effective as the inspection protocols in place. (FOF ¶ 1087.) Indeed, it is fair to say that the only function of seals is to be inspected. (FOF ¶ 1087.) Effective inspections take account of the unique properties and vulnerabilities of each particular seal; in order for that to happen, they must be governed by carefully

submission that will be redacted from the public version of this submission.

thought-out protocols. (FOF ¶ 1087.)

5. The State Administers Elections Without Consulting Any Professional Security Experts, Resulting In Systemic Vulnerabilities.

Dr. Johnston testified that in developing a healthy security culture, it is essential to seek advice from on-staff and external security experts. (FOF ¶ 1088.) New Jersey has no on-staff security experts, and has consulted no physical security experts. (FOF ¶ 1088.) Instead, the State has relied exclusively upon the manufacturers of the seals for security advice, particularly the Brooks Company. (FOF ¶ 1088.) The conflict of interest should be obvious: a seal manufacturer has a financial interest in selling seals. This does not take into account the security interests of its clients. (FOF ¶ 1088.) Indeed, seals that Mr. Giles testified were recommended by Brooks as being foolproof were defeated by both Dr. Johnston and Professor Appel. (FOF ¶ 1088.)

6. Mr. Giles' Lack of Understanding of Security Issues Exacerbates the Vulnerabilities of New Jersey's DRE's.

According to Dr. Johnston, the fact that Mr. Giles, the Director of the Division of Elections, does not understand physical or cyber security illustrates New Jersey's poor security culture. (FOF ¶ 1089.) Dr. Johnston's expert reports emphasize that security depends crucially on organizational security culture and priorities. (FOF ¶ 1089.) As Director of the Division of Elections, Mr. Giles' own attitudes and understanding have a tremendous affect on New Jersey's election security. (FOF ¶ 1089.)

After reading Mr. Giles' deposition, Dr. Johnston concluded that "[i]n my professional opinion, Mr. Giles' views represent major barriers to having good election integrity, and show evidence of an unhealthy security culture." (FOF ¶ 1090.)

Dr. Johnston identified even more indicators of poor security culture in New Jersey by examining the depositions of James Clayton of Ocean County, Elisa Gentile of Hudson County, and

Daryl Mahoney of Bergen County. (FOF ¶ 1093.) He laid special emphasis on security vulnerabilities in the transport, storage, and delivery of DREs. (FOF ¶ 1093.) These flaws create genuine security vulnerabilities. (FOF ¶ 1093.) On the basis of his research, and after reading the depositions of the witnesses named directly above, Dr. Johnston's conclusion is that

> [g]iven limited security features built into the AVC Advantage voting machine, the absence of a healthy security culture for New Jersey elections, and New Jersey's lack of well designed seal use protocols, I believe there are viable attacks on New Jersey voting machines that are . . . capable of affecting election results.

(FOF ¶ 1094.) New Jersey's poor security culture creates the possibility that an election may be stolen. (FOF ¶ 1094.)

Dr. Johnston testified about objective research demonstrating that a poor attitude toward security results in vulnerabilities. (FOF ¶ 1095.) Dr. Johnston has published articles in industrial/organizational psychology journals on this "cognitive dissonance," and has supervised a Ph.D. thesis on the subject. (FOF ¶ 1095.) He has shown that statistically significant correlations exist indicating that attitudes towards security are powerful predictors of security problems. (FOF ¶ 1095.) New Jersey's unhealthy security culture, in other words, is itself an indicator that State elections are vulnerable to attack. (FOF ¶ 1095.)

C. ALL OF THE SEALS PROPOSED BY THE STATE ARE READILY DEFEATED WITH LITTLE EXPERTISE, MONEY, OR TECHNOLOGY.

During both direct and cross examination, Dr. Johnston demonstrated to the Court that simple, low-tech, inexpensive methods exist for defeating all of New Jersey's proposed seals. (FOF ¶ 1096.) Further, he demonstrated attacks requiring no expertise beyond that of a high-school-age hobbyist. (FOF ¶ 1096.)

1. During His Direct Testimony Dr. Johnston Demonstrated The Successful Defeat Of All The Security Measures Proposed By The State.

Dr. Johnston defeated all of the seals contemplated by the State, in open court. He defeated seals provided to him in early 2009, as well as seals that the State proposed for use months after trial began. (FOF ¶ 1097.) The State's seals changed repeatedly and continued to change until April 2008, days before Dr. Johnson testified. With little notice, Dr. Johnston devised successful defeats for all of the seals he was given, in a very short time. (FOF ¶ 1097.)

The attacks Dr. Johnston demonstrated are only the tip of the iceberg. (FOF ¶ 1098.) Dr. Johnston testified that it is essential to take seriously every feasible attack that can be conceived, even if it has not been demonstrated. (FOF ¶ 1098.) According to Dr. Johnston, security vulnerabilities are unlimited. (FOF ¶ 1098.) Assessing vulnerability, as Dr. Johnston testified, is about identifying the vulnerabilities most likely to be exploited, and addressing those that can be fixed. (FOF ¶ 1098.)

Just as it is crucial to take every conceivable attack seriously, it is crucial to take every possible attacker seriously. (FOF ¶ 1099.) An attacker need not have a Ph.D. to devise and successfully implement an attack. (FOF ¶ 1099.) In fact, Dr. Johnston reported that in his experience, "the average laboratory technician, auto mechanic, artist, crafts person, or wood worker can master attacks on seals more quickly than Ph.D.'s and can demonstrate better mechanical proficiency." (FOF ¶ 1099.) According to Dr. Johnston, his team of technicians and students at Argonne National Laboratory define attacks as "especially easy" if Dr. Johnston can perform them. (FOF ¶ 1099.)

Dr. Johnston's courtroom demonstrations prove beyond any doubt that it is possible to defeat all of New Jersey's proposed seals. (FOF ¶ 1100.) They represent only a small subset of the possible methods for hacking into the State's DREs. (FOF ¶ 1100.) Notably, the time it took Dr. Johnston to defeat the seals is not in any way indicative of how long someone with more practice and with good manual dexterity would take to defeat the seals. (FOF ¶ 1100.)

a. Brooks Padlock Seal

The Brooks Padlock seal is a padlock with three components: a clear plastic housing containing a blue plastic body; and an arched, steel shackle that clips into the blue body just like a padlock shackle. (FOF ¶ 1101.) The blue plastic body on each Brooks Padlock Seal is marked with an adhesive label bearing a serial number with a barcode. (FOF ¶ 1101.) Once the shackle is engaged, it is not supposed to be removable without destroying the seal. (FOF ¶ 1101.) Dr. Johnston demonstrated two methods for defeating this seal:

[redacted]

Dr. Johnston uses the term "partial counterfeit" to describe this attack, because he uses parts of the real seal to produce the counterfeit. (FOF ¶ 1102.)

[redacted]

Samples of the Brooks Padlock Seal are readily available to the general public. (FOF ¶ 1103.) Brooks distributes free samples upon request, and sells large quantities at low cost. (FOF ¶ 1103.) As a result, an attacker is easily able to acquire Padlock Seals to dismantle for spare parts or practice attacks. (FOF ¶ 1103.) Dismantling the seals is a simple matter; Dr. Johnston testified that an attacker could dismantle seals at his leisure, even while watching TV. (FOF ¶ 1103.)

Another method for defeating the Brooks Padlock Seal is to make a counterfeit seal bearing the same serial number. (FOF ¶ 1104.) This method produces a full counterfeit, since no parts of the real seal are used. (FOF ¶ 1104.) [redacted] (FOF ¶ 1104.) Armed with counterfeit seals, an attacker need merely cut off the original seal and substitute a counterfeit, a seconds-long operation. (FOF ¶ 1104.)

Dr. Johnston brought seven such counterfeit Padlock Seals with him to court. (FOF ¶ 1105.) They were admitted into evidence as Exhibit P-88. (FOF ¶ 1105.) He was able to manufacture the counterfeits literally on the eve of trial, among all his other preparations, using one of the Plaintiffs' home printer. (FOF ¶ 1105.) He presented the seven counterfeits along with one original, all bearing the same serial number, to the Court and Defendants' counsel for inspection one at a time. (FOF ¶ 1105.) Neither the Court nor Defendants' counsel were able to distinguish the genuine seal from the counterfeits, nor one seal from another. (FOF ¶ 1105.)

Dr. Johnston presented the seals to the Court one at a time in order to simulate actual inspection conditions. (FOF ¶ 1106.) In the real world, seal inspectors examine seals one at a time. (FOF ¶ 1106.) They often work in poor lighting. (FOF ¶ 1106.) Unlike in the courtroom setting, real inspectors are not given advance warning that a seal has been counterfeited, and thus may lack motivation. (FOF ¶ 1106.) They do not have a counterfeit and a legitimate seal to compare during inspections, but must evaluate only what is before them. (FOF ¶ 1106.)

Moreover, seal inspections cannot be effective in an unhealthy security culture. Johnston Test., (FOF ¶ 1107.) Detecting a counterfeit is practically impossible without detailed protocols structured to address the specific vulnerabilities of the seal. (FOF ¶ 1107.) Unless seals are inspected under carefully conceived protocols, according to Dr. Johnston, an attacker could steal votes without being detected. (FOF ¶ 1107.) As Dr. Johnston put it, given New Jersey's nonexistent use protocols, "the most minimal of effort will constitute a defeat." (FOF ¶ 1107.)

b. Brooks Padlock Seal With Gorilla Glue

After learning of Dr. Appel's success defeating the Brooks Padlock Seal in December 2008, the State proposed adding Gorilla Glue to the seal. (FOF ¶ 1108.) The State proposes to inject the Gorilla Glue into the hole where the shackle engages, on the theory that the glue will hold the seal together, preventing the kinds of simple defeats identified by Dr. Johnston. (FOF ¶ 1108.)

Dr. Johnston was easily able to defeat the glued Brooks Padlock Seal. (FOF ¶ 1109.) It was a simple matter of producing a counterfeit as described above and then adding Gorilla Glue before engaging the shackle. (FOF ¶ 1109.) In Dr. Johnston's terminology, this is a full counterfeit, as it is made entirely from fresh materials. (FOF ¶ 1109.) Dr. Johnston successfully produced glued counterfeits in Court, which were admitted into evidence as Exhibit P-89. (FOF ¶ 1109.) He testified that adding the Gorilla Glue has the opposite effect of what Defendants intended. (FOF ¶ 1109.) It makes the seals less secure. (FOF ¶ 1109.)

The Gorilla Glue leaves marks on the Brooks Padlock Seals that, in Dr. Johnston's opinion, are likely to lead inspectors to make incorrect determinations. (FOF ¶ 1110.) When the Gorilla Glue is injected into the clear plastic housing and the shackle is engaged, it flows throughout the clear plastic housing and across the serial number label in unpredictable patterns. (FOF ¶ 1110.) As noted above, the key to tamper-indicating seals is predictability. (FOF ¶ 1110.) The glue flow patterns make every seal look different in ways that are meaningless to inspectors unless a photograph is taken of every single seal. (FOF ¶ 1110.) If the glue is injected in both sides, the random effect is twice as bad. (FOF ¶ 1110.) The State's poor understanding of the proposal to add Gorilla Glue to the Brooks Padlock Seals illustrates how its unhealthy security culture fails to protect the DREs from attack. (FOF ¶ 1110.)

c. American Casting And Manufacturing Small Cup "Seal"

The American Casting and Manufacturing (ACM) Small Cup Seal is fundamentally a device meant to protect the screws on New Jersey's DREs from being opened with an ordinary screwdriver. (FOF ¶ 1111.) The Small Cup "Seal" consists of two parts: a cup with a hole in it through which the screw is inserted, and a cap that snaps onto the cup. (FOF ¶ 1111.) Once the cap is attached, the head of the screw is theoretically inaccessible, supposedly converting the screw into a robust security seal. (FOF ¶ 1111.)

But, the Small Cup "Seal" is not a seal at all! It lacks any unique identifier, a critical aspect of tamper-indicating seals. (FOF ¶ 1112.) Additionally, the three-eighths-inch device chosen by New Jersey is no longer manufactured by ACM. (FOF ¶ 1112.) It does not come engraved with serial numbers. (FOF ¶ 1112.) Without a serial number, the device lacks any unique identifier, and does not qualify as a tamper-indicating seal under the most basic definition. (FOF ¶ 1112.) Each and every Small Cup "Seal" is identical, making it impossible to detect a swap. (FOF ¶ 1112.)

Even if serial numbers are added to the Small Cup "Seals," the serial numbers will be too difficult to read to offer any effective security. (FOF ¶ 1113.) The Small Cup "Seal" is very small, so the serial number printed on it would necessarily be even smaller. (FOF ¶ 1113.) Even under good illumination conditions, Dr. Johnston testified that the numbers will be very difficult read. (FOF ¶ 1113.) He testified that the location of the seals made the Small Cup "Seals" even harder to read. (FOF ¶ 1113.) His conclusion, based on past experience, was that seal inspectors will not do a good job on seals that are difficult to inspect. (FOF ¶ 1113.) Even if the Small Cup "Seal" were a legitimate tamper-indicating security seal marked with a serial number, they would still not afford effective security. (FOF ¶ 1113.)

The fact that ACM no longer manufactures the Small Cup "Seal" renders the device meaningless from a security perspective. (FOF ¶ 1114.) The State proposes to install the Small Cup "Seals" in three locations on the DREs: underneath the audio cartridge; on the power panel; and in the upper-left corner of the metal cover. (FOF ¶ 1114.)

With 11,000 DREs in use in New Jersey, the State will need to install 33,000 Small Cup "Seals" at the outset. (FOF ¶ 1115.) Further, large quantities of the seals are needed as examples to train installers and inspectors. (FOF ¶ 1115.) It is also important for inspectors to witness demonstration attacks on real seals, which usually cannot be re-used afterwards. (FOF ¶ 1115.) All of these activities will diminish the existing supplies of the device. (FOF ¶ 1115.) Dr. Johnston had no trouble ordering approximately sixty sample Small Cup "Seals" from ACM, further diminishing the number available to New Jersey. (FOF ¶ 1115.)

The Small Cup "Seal" can be easily defeated. [redacted] ¶ 1116.) Dr. Johnston was able to complete the attack within thirty seconds. (FOF ¶ 1116.) More facile members of his team were able to complete it within three to ten seconds. (FOF ¶ 1116.) The cost of the attack is negligible given the stakes: [redacted] (FOF ¶ 1116.) The attack does not damage the seal, which can be reused, making the attack all but undetectable. (FOF ¶ 1116.)

Dr. Johnston is able to defeat the Small Cup "Seals," even if serial numbers are added. (FOF ¶ 1117.) [redacted] (FOF ¶ 1117.) An With such a machine, an attacker could gain unhampered access to the inner workings of New Jersey's DREs. (FOF ¶ 1117.)

d. American Casting And Manufacturing Large Cup Seal

In his testimony, Dr. Johnston described two attacks that defeat the Large Cup Seal also manufactured by ACM. Like the Small Cup Seal, the Large Cup Seal comprises a bottom cup and a top cap that snaps on. (FOF ¶ 1118.) The cap snaps on with "leaf-spring fingers" that hold it in place. (FOF ¶ 1118.)

Dr. Johnston's first attack is the same as his attack on the Small Cup Seal: [redacted] (FOF ¶ 1119.) Dr. Johnston is able to perform this attack within 90 seconds; technicians on his Vulnerability Assessment Team are able to perform it within 10 seconds. (FOF ¶ 1119.)

In Dr. Johnston's second attack, [redacted] This attack can easily be completed in a way that is difficult to detect. (FOF ¶ 1120.)

Dr. Johnston testified that Professor Appel's attack on this seal would also successfully defeat it. (FOF ¶ 1121.)

Both of these attack methods produce partial counterfeits, since parts of the original Cup Seals remain in place. (FOF ¶ 1122.)

e. American Casting And Manufacturing Small and Large Cup Seals With Gorilla Glue

The State has also proposed adding Gorilla Glue to the Cup Seals in response to the defeats Professor Appel demonstrated in court and to the defeats discussed in Dr. Johnston's expert report. (FOF ¶ 1123.) This measure actually made the seal easier for Dr. Johnston to defeat. (FOF ¶ 1123.)

This new measure is problematic in many ways. (FOF ¶ 1124.) In Dr. Johnston's courtroom demonstration (Exhibit P-102), the Gorilla Glue stuck the parts of the Cup Seals together. (FOF ¶ 1124.) As a result, Dr. Johnston was able to remove the seals like normal screws, simply by turning the whole apparatus, by hand! (FOF ¶ 1124.) He glued the top cap of each seal to the bottom cup, attempting not to fill the whole cavity. (FOF ¶ 1124.) Although he made every effort to apply the Gorilla Glue consistently, he found that the Gorilla Glue is by its nature unpredictable. (FOF ¶ 1124.)

Moreover, the application of the glue itself causes serious problems for inspectors. (FOF ¶ 1125.) The Gorilla Glue shrinks as it cures, pulling on the surface of the top cap and causing dimples to appear unpredictably. (FOF ¶ 1125.) The presence of unpredictable damage on genuine seals makes it easier to mask an actual attack. (FOF ¶ 1125.)

The glue proposed by the State is a cyanoacrylate, a hazardous chemical with serious environmental and health effects. (FOF ¶ 1126.) Dr. Johnston consulted the Material Safety and Data Sheet for cyanoacrylates, which states that "[cyanoacrylate adhesive] . . . bonds with human tissue including skin in seconds." (FOF ¶ 1126.) Further, when a cyanoacrylate like Gorilla Glue comes in contact with clothing or human tissue, it "will generate heat causing smoke, sun burns and strong irritating vapors." (FOF ¶ 1126.) Any worker responsible for gluing hundreds of seals would face prolonged exposure. (FOF ¶ 1126.) New Jersey has not addressed the potential OSHA issues arising from these hazards. (FOF ¶ 1126.)

f. Plastic Strap Seals

The State has also introduced a Plastic Strap Seal manufactured by Electek. (FOF ¶ 1127.) Dr. Johnston defeated the seal on his first attempt, after spending a mere ten minutes examining it. (FOF ¶ 1127.) Dr. Johnston has shown how to pick open strap seals with everyday materials, in a matter of seconds. (FOF ¶ 1127.)

The Plastic Strap Seal is based on a ratchet principle: the seal's toothed plastic strap slides into a plastic body, where the teeth engage with a locking mechanism. (FOF ¶ 1128.) [redacted] This attack leaves the seal undamaged: an attacker would simply replace the original seal, making the attack undetectable. (FOF ¶ 1128.)

Dr. Johnston's [redacted] is widely known and discussed among hobbyists on the Internet. (FOF ¶ 1129.) The only equipment needed to successfully perform the attack is [redacted]

Dr. Johnston was also able to defeat the Plastic Strap Seal [redacted] (FOF ¶ 1130.) This attack is the same in principle as [redacted] (FOF ¶ 1130.) With little expertise or expense, according to Dr. Johnston, an attacker can defeat the Plastic Strap seals, potentially changing election outcomes. (FOF ¶ 1130.)

g. Brooks Red Adhesive Tape Seal

(i) Brooks Red Adhesive Tape Installation Problems

The Red Tape Seal suffers from serious flaws that increase its cost to the State, and its vulnerability to attack. (FOF ¶ 1131.) The adhesive substrate is so strong that the seals are very difficult to remove from the rolls on which they are shipped. (FOF ¶ 1131.) The plastic top layer tends to separate from the substrate on removal from the roll, causing damage to the edges and exposing the "void, opened" marks on the substrate. (FOF ¶ 1131.) These damaged seals are irreparable and unusable, resulting in numerous wasted seals at great expense to the taxpayers. (FOF ¶ 1131.)

Dr. Johnston examined photographs taken by Professor Appel of the Red Tape Seal applied to the DREs. (FOF ¶ 1132.) He testified that the inconsistent installation results inherent to the Red Tape Seal make it easier for attackers to defeat the seals. (FOF ¶ 1132.)

For example, the Red Tape Seal leaves marks wherever it is applied, so that if an installer fails to lay the seal down correctly on the first attempt, he will leave a mess of glue around the seal. (FOF ¶ 1133.) Dr. Johnston observed this kind of damage in Professor Appel's photograph of the Red Tape Seal on the DRE audio cartridge, which had damage to the upper-left corner and upper edge. (FOF ¶ 1133.) He concluded that a close-up of the same Red Tape Seal revealed adhesive on the surface around the seal deposited during the installation process. (FOF ¶ 1133.)

This kind of damage compromises the efficacy of the seal. (FOF ¶ 1134.) The likelihood that seals will appear damaged tends to lead inspectors either to erroneously identify tampering, or to learn to expect damage; Dr. Johnston concludes that these flaws open New Jersey's DREs to attack. (FOF ¶ 1134.)

Dr. Johnston also testified that the Red Tape Seal installed on the left side of the DRE had a bubble in the lower-right corner. (FOF ¶ 1135.) He testified that the bubble could be an indication of an attack, but in this case was the result of the difficulty of installing the Red Tape Seal. (FOF ¶ 1135.) In his opinion, the Red Tape Seals, as demonstrated in the photographs taken by Professor Appel would lead to a false positive: an inspector would erroneously report an attack. (FOF ¶ 1135.)

The occurrence of false positives drastically undercuts the efficacy of a seals program. (FOF ¶ 1135.) Indeed, inspectors who expect to see routine damage will overlook evidence of an attack. (FOF ¶ 1135.) The seal that "cries wolf" is not an effective guard. (FOF ¶ 1135.)

(ii) Brooks Red Adhesive Tape Seal Clean Up Problems

The messiness of the Red Tape Seal also requires time-consuming clean-up, further compromising its efficacy. (FOF ¶ 1136.) As discussed earlier, the Red Tape Seal leaves behind its adhesive substrate when removed. (FOF ¶ 1136.) But the seal will only adhere correctly to a clean surface. (FOF ¶ 1136.) Thus, every time a Red Tape Seal is removed, the substrate must be cleaned off before a replacement can be applied. (FOF ¶ 1136.) When Dr. Johnston demonstrated the cleaning process for the Court, it took him twelve minutes. (FOF ¶ 1136.)

To clean off the gunk, Dr. Johnston had to use solvents that give off toxic fumes. (FOF ¶ 1137.) In fact, when Dr. Johnston was cleaning off the gunk in the courtroom, the court reporter asked and was granted permission to exit the courtroom for the duration of the demonstration, because she could not endure the powerful, toxic fumes. (FOF ¶ 1137.) Dr. Johnston testified that the solvent he used causes harm to health from long-term exposure. (FOF ¶ 1137.) The solvent, which Dr. Johnston testified has much the same effects as other solvents, is labeled with the following warnings:

> Danger: harmful or fatal if swallowed. Contains acetone, xylene, ethyl benzene, butyl carbitol, petroleum distillates, and toluene. Contact physician immediately. Do not induce vomiting. Avoid prolonged contact with skin. Do not get in eyes. In case of eye contact, flush with water for 15 minutes. . . . [E]xtremely flammable liquid and vapor. Vapor harmful or fatal if swallowed.

(FOF ¶ 1137.) Dr. Johnston testified that in order to clean the adhesive from all of its DREs, New Jersey would have to buy dangerous solvents in 55-gallon drums. (FOF ¶ 1137.)

Since the State proposes to use the Red Tape Seals in two locations on the DREs, an inspector would have to spend twelve minutes exposed to the fumes for every seal he removed. (FOF ¶ 1138.) That adds up to twenty-four minutes per DRE. (FOF ¶ 1138.) Many counties have hundreds of DREs. (FOF ¶ 1138.)

Any maintenance person changing a battery or even checking to see if the EPROMs have been tampered with would suffer the same harmful exposure. (FOF ¶ 1139.) Workers responsible for removing, inspecting, and installing hundreds or thousands of seals would ultimately spend hundreds of hours exposed to dangerous chemicals, causing serious harm to their health. (FOF ¶ 1139.)

After more than seventeen years leading the most respected teams in the field, Dr. Johnston concluded that if it is difficult to inspect a seal, inspectors will not do a thorough job. (FOF ¶ 1140.) A seal inspector asked to spend twenty-four minutes per machine cleaning gunk and breathing toxic fumes will not do a good enough job to protect New Jersey's DREs from attack. (FOF ¶ 1140.)

(iii) Attack on Brooks Red Adhesive Tape Seal

The Brooks Red Pressure-Sensitive Adhesive Tape Seal (Red Tape Seal) comprises two parts: an adhesive substrate, and a red plastic top layer. (FOF ¶ 1141.) The adhesive substrate bears the words "void" and "opened." (FOF ¶ 1141.) The two words remain behind when the seal's top layer is removed, providing tamper indication. (FOF ¶ 1141.)

In one corner of the substrate, a unique serial number is printed. (FOF ¶ 1142.) The plastic top layer has a clear window in the same location through which the serial number is visible. (FOF ¶ 1142.) But when the plastic top layer is removed, the serial number stays behind on the adhesive substrate. (FOF ¶ 1142.)

Exploiting this characteristic, Dr. Johnston demonstrated a straightforward method for defeating the Red Tape Seal:

[redacted]

Since the original serial number remains in place, this attack is a partial counterfeit. (FOF ¶ 1144.) The strength of the attack is that the defeated seal behaves just like a normal one; the attack is undetectable without sophisticated chemical forensics. (FOF ¶ 1144.) The total cost of the equipment for this attack was between $7 and $9, according to Dr. Johnston. (FOF ¶ 1144.)

h. Brooks Small MRS2 Pressure-Sensitive Adhesive Seal

Dr. Johnston testified that pressure-sensitive adhesive seals like the Small Brooks MRS2 Seal do not provide effective security. (FOF ¶ 1145.) In fact, the Small Brooks MRS2 Seal is "even easier to defeat than many other [pressure-sensitive adhesive] seals." (FOF ¶ 1145.) This is because the seal's adhesive is weak, making it easy to lift off the of the DRE. (FOF ¶ 1145.)

Dr. Johnston also testified that it is easy to counterfeit the Small Brooks MRS2 Seal using inexpensive, low-tech equipment. (FOF ¶ 1146.) Each seal has a unique serial number printed on it. (FOF ¶ 1146.) Dr. Johnston uses the following method to produce a full counterfeit:

[redacted]

[redacted]

Dr. Johnston testified that using solvents to attack adhesive-tape seals is a well-known attack method. (FOF ¶ 1147.) For at least three decades, according to Dr. Johnston, people have been discussing this method of attacking adhesive-tape seals like the Small Brooks MRS2 Seal on the internet. (FOF ¶ 1147.) Dr. Johnston testified that numerous government reports dating back to the 1970s document the vulnerability of pressure-sensitive adhesive seals to solvents. (FOF ¶ 1147.)

This kind of attack is so well known that it only took Dr. Johnston two minutes to figure out how to defeat the Small Brooks MRS2 Seal. (FOF ¶ 1148.)

Dr. Johnston testified that it is simple to produce a counterfeit MRS2 serial number. (FOF ¶ 1149.) [redacted] (FOF ¶ 1149.) The Small Brooks MRS2 Seal has no bar code, making it even easier to produce a full counterfeit. (FOF ¶ 1149.)

Often, according to Dr. Johnston, one can order specific serial numbers from seal manufacturers. (FOF ¶ 1150.) An attacker may be able to order a range of custom serial numbers from Brooks. (FOF ¶ 1150.) With counterfeits made to order by the manufacturer, an attacker would have an even easier time installing vote-stealing software on New Jersey's DREs. (FOF ¶ 1150.)

No special expertise is needed to perform this attack. (FOF ¶ 1151.) An attacker with access [redacted] counterfeit. (FOF ¶ 1151.)

Dr. Johnston brought five counterfeit Small Brooks MRS2 Seals with him to court. (FOF ¶ 1152.) They were admitted into evidence as Exhibit P-90. (FOF ¶ 1152.) Like the Brooks Padlock Seal, Dr. Johnston was able to manufacture counterfeit Small Brooks MRS2 Seals on the eve of trial. (FOF ¶ 1152.) He presented the five counterfeits along with one original, all bearing the same serial number, to the Court and Defendants' counsel for inspection one at a time. (FOF ¶ 1152.) Neither the Court nor Defendants' counsel were able to distinguish the genuine seal from the counterfeits, nor one seal from another. (FOF ¶ 1152.)

Again, presenting seals to the Court one at a time simulates actual inspection conditions, according to Dr. Johnston. (FOF ¶ 1153.) A real seal inspector examines seals one at a time, with no warning that an attack has taken place, and with no opportunity to examine an attacker's different attempts. (FOF ¶ 1153.)

Dr. Johnston testified further that more high-tech methods exist for defeating the Small Brooks MRS2 Seal. (FOF ¶ 1154.) For example, the vinyl material that the seal is made of is also used in standard vinyl tape, available at grocery and hardware stores. (FOF ¶ 1154.) [redacted] (FOF ¶ 1154.) An advanced attack like this could defeat even a relatively advanced seal use protocol. (FOF ¶ 1154.) Materials are readily available to make high-quality counterfeits of the Small Brooks MRS2 Seal, making New Jersey's DREs vulnerable to vote-stealing attacks. (FOF ¶ 1154.)

i. Brooks Small MRS2 Pressure-Sensitive Adhesive Seal with Ultraviolet Markings

The Brooks small MRS2 seal produced by the state does not exist with an ultraviolet mark of logo. (FOF ¶ 1077.) Dr Johnston testified that, to his understanding, Brooks has merely discussed providing the Small MRS2 seal with an ultraviolet mark as an option, but no such seal is currently on production. (FOF ¶ 1077.)

Although it is very difficult to assess the viability of a seal that does not exist (FOF ¶ 1077), the use of ultraviolet marks or logos is quite common and goes back many decades. (FOF ¶ 1047.) Indeed, the use of an ultraviolet mark on a seal is "probably the most obvious thing anyone looking at a seal trying to see if there was some anti-counterfeit feature would think about." (FOF ¶ 1159.)

Spotting an ultraviolet mark on a seal is as simple as shining an ultraviolet flashlight on a seal. (FOF ¶ 1160.) By examining the seals initially for ultraviolet markings, an attacker could decide whether he wanted to counterfeit the marking or whether he wanted to attack the seal in such a way that did not disturb the ultraviolet portion. (Id.)

Counterfeiting an ultraviolet mark is essentially no different than counterfeiting a visible ink mark. (FOF ¶ 1161.) [redacted] (FOF ¶ 1161.) [redacted] (FOF ¶ 1161.) The Seal of the State of New Jersey is readily available on the State's website. (FOF ¶ 1161.)

The materials needed to counterfeit a seal with an ultraviolet logo are readily available to consumers on the Internet. (FOF ¶ 1162.) [redacted] (Id.)

An attacker does not have to recreate the logo with precision because one of the advantages (to an attacker) of an ultraviolet image is that it is difficult to see. (FOF ¶ 1163.) If the ultraviolet image has roughly the same shape and approximately the same fluorescent color. Then it will typically be accepted by the seal inspector as an indication of the ultraviolet mark, and hence not counterfeit. (FOF ¶ 1163.)

The method in which the state proposes to use the ultraviolet seals would assist an attacker.

The State proposes to use ultraviolet seals bent across the ROM chips on the motherboard. This makes the seals very difficult to inspect. (FOF ¶ 1164.)

Dr. Johnston testified that ultraviolet markings do not represent any significant extra security feature, and do not increase the tamper detection reliability of a seal. (FOF ¶ 1165.)

j. Brooks Large MRS2 Pressure-Sensitive Adhesive Seal

New Jersey also proposes to use a larger version of the Brooks MRS2 Seal. (FOF ¶ 1155.) Dr. Johnston testified that the Large Brooks MRS2 Seal is fundamentally the same as the Small Brooks MRS2 Seal. (FOF ¶ 1155.) He testified, further, that he is able to defeat the Large Brooks MRS2 Seal using the same technique as the Small Brooks MRS2 Seal. (FOF ¶ 1155.) He is able to manufacture a partial counterfeit of the Large Brooks MRS2 Seal [redacted]

Dr. Johnston testified that the Large Brooks MRS2 Seal has a rectangular box printed on it, for seal installers to add their signatures. (FOF ¶ 1156.) New Jersey does not use this feature; it installs the Large Brooke MRS2 Seal without a signature. (FOF ¶ 1156.) Adding a signature to the seal, according to Dr. Johnston, would make a counterfeiting attack somewhat more complicated. (FOF ¶ 1156.) Although Dr. Johnston testified that adding a signature would not substantially improve the Large Brooks MRS2 Seal's security, the fact that the State has ignored this feature is further evidence of its poor security culture. (FOF ¶ 1156.)

2. On Cross Examination Dr. Johnston Again Defeated All of the Security Measures Proposed By The State In Ways That Avoid Detection

On cross examination, Dr. Johnston was asked to defeat all of the seals that were placed by Mr. Giles on the Sequoia AVC Advantage DRE that was in the State's custody. (FOF ¶ 1166.) He defeated all of the seals. (FOF ¶ 1166.)

Dr. Johnston testified at length concerning the poor likelihood that seal inspectors would detect the attacks of New Jersey's proposed seals that he demonstrated. (FOF ¶ 1167.) At the Court's request, Dr. Johnston testified about three different levels of security protocols, Level 1, Level 2, and Level 3, and when his attacks would be detected using each level of security protocol. (FOF ¶ 1167.)

Level 1, the level in use in New Jersey, is no seal use protocol, no plan for inspections, and no training on attacks or understanding of attack methods. (FOF ¶ 1168.)

Level 2 is some kind of seal use protocol, with modest training on the protocol for seal installers and inspectors. (FOF ¶ 1169.)

Level 3, the highest level, is a very effective seal use protocol combined with extensive training. (FOF ¶ 1170.) In reality, implementing Level 3 protocols is so complex and expensive that they are almost never used. (FOF ¶ 1170.) Dr. Johnston testified that even nuclear safeguards rarely use Level 3 protocols. (FOF ¶ 1170.) Further, he testified that his Vulnerability Assessment Team has found it a very difficult challenge to develop Level 3 protocols. (FOF ¶ 1170.) Forensic lab results of the kind required for Level 3 protocols can take weeks to obtain. (FOF ¶ 1170.) The extreme cost and complexity of Level 3 protocols makes them all but nonexistent in practical applications. (FOF ¶ 1170.)

Dr. Johnston's conclusions about the efficacy of different protocol levels on each seal are as follows:

- **Brooks Padlock Seal with Gorilla Glue**: Dr. Johnston defeated this seal by making and installing a counterfeit bearing the same serial number as the Brooks Padlock Seal installed on the DRE by the State. New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (FOF ¶ 1171.)

> Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check. (FOF ¶ 1172.) This would not detect his attack on the Brooks Padlock Seal with Gorilla Glue, or any comparable attack. (FOF ¶ 1172.)
>
> Level 2: Level 2 protocols for the Brooks Padlock Seal would likely include more careful visual inspection, and some tactile examination. (FOF ¶ 1173.) Level 2 protocols would not detect Dr. Johnston's attack on the Brooks Padlock Seal with Gorilla Glue. (FOF ¶ 1173.)
>
> Level 3: Level 3 protocols would involve disassembling the seal and carefully studying the individual components under a microscope. (FOF ¶ 1174.) Level 3 would detect an attack. But, according to Dr. Johnston, detection would be extraordinarily expensive. (FOF ¶ 1174.)

- **Large and Small Brooks MRS2 Tape Seals**: Dr. Johnston produced a partial counterfeit of the Small Brooks MRS2 Seal. (FOF ¶ 1174.) [redacted] (FOF ¶ 1174.) Dr. Johnston testified that he defeated the Large Brooks MRS2 Seal using the same method. (FOF ¶ 1174.) New Jersey currently has no use protocols in place for the Large or Small Brooks MRS2 Seals, putting it at Level 1. (FOF ¶ 1174.)

> Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check on the Large and Small Brooks MRS2 Seals. (FOF ¶ 1175.) This would not detect his attack on the Large or Small MRS2 Seals, or any comparable attack. (FOF ¶ 1175.)
>
> Level 2: Dr. Johnston testified that at best, Level 2 protocols for the Large and Small Brooks MRS2 Seals would involve outstanding training and highly motivated installers. (FOF ¶ 1176.) Nonetheless, Dr. Johnston concluded that the odds of detecting his attack on the Large and Small Brooks MRS2 Seals with Level 2 protocols are at best 50%. (FOF ¶ 1176.)
>
> Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, Level 3 protocols would involve expensive and complex forensic examination of the seal's chemical makeup. (FOF ¶ 1177.) Such detailed examination is, again, prohibitively complex and costly. (FOF ¶ 1177.)

- **Brooks Red Adhesive Tape Seal**: Dr. Johnston defeated this seal using a partial counterfeit, [redacted] (FOF ¶ 1177.) New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (FOF ¶ 1177.)

> Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check. (FOF ¶ 1178.) This would not detect his attack on the Brooks Red Adhesive Tape Seal, or any comparable attack. (FOF ¶ 1178.)
>
> Level 2: To qualify as Level 2, protocols would have to devote attention both to the serial number and to any damage inflicted during installation. (FOF ¶ 1179.) This With careful training and motivated staff, Dr. Johnston testified Level 2 protocols would have a 50% chance of detecting his attack. (FOF ¶ 1179.)
>
> Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, Level 3 protocols would involve disassembling the Brooks Red Tape Seal and analyzing the chemicals on the underside of the tape. (FOF ¶ 1180.) Performing such detailed analysis on 11,000 DREs would be prohibitively complex and costly. (FOF ¶ 1180.)

- **American Casting and Manufacturing Metal Cup Seals With Gorilla Glue**: Dr. Johnston was able to simply unscrew these seals by hand after the Gorilla Glue stuck the whole assembly together. (FOF ¶ 1180.) Dr. Johnston testified that since he is able to remove and put the original Cup Seals back in their original locations, neither Level 1 nor Level 2 protocols would detect his attack on the Cup Seals with Gorilla Glue, or any comparable attack. (FOF ¶ 1180.)

> Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, such a protocol for this seal would be enormously expensive and complex. (FOF ¶ 1181.) Inspectors would have to take microphotographs of the seals at installation, and compare them with new microphotographs taken during inspection to detect otherwise invisible marks left by an attacker. (FOF ¶ 1181.) Like the other Level 3 protocols, this is too costly and complex for New Jersey to implement. (FOF ¶ 1181.)

Dr. Johnston found that in one instance the glue stuck the entire seal to the sheet metal of the DRE, turning it into a lock, rather than a seal. (FOF ¶ 1182.) Dr. Johnston was able to completely remove the seal with bolt cutters and replace it with an identical cup seal. (FOF ¶ 1182.)

Converting cup seals into locks using gorilla glue is very problematic. As mentioned earlier, tamper-indicating seals only work when their appearance and behavior are predictable. (FOF ¶ 1183.) In the case of Cup Seals that adhere to the DRE, inspectors trying to remove the devices are prone to causing unpredictable damage to the DRE likely to result in false positives during inspections. (FOF ¶ 1183.) When this happens, in Dr. Johnston's expert opinion, inspectors come to expect false positives; as a result, they learn to ignore damaged seals. (FOF ¶ 1183.) As a result, they ignore evidence of real attacks. (FOF ¶ 1183.)

- **<u>Plastic Strap Seals</u>**: Dr. Johnston picked open the Plastic Strap Seals [redacted] (FOF ¶ 1183.) New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (FOF ¶ 1183.)

  > <u>Level 1</u>: Dr. Johnston concluded that without use protocols, an inspector would not detect his attack on the Plastic Strap Seals, or any comparable attack. (FOF ¶ 1184.)
  >
  > <u>Level 2</u>: A Level 2 protocol would, in Dr. Johnston's opinion, stand at best a 50% chance of detecting his attack. (FOF ¶ 1185.)
  >
  > <u>Level 3</u>: Although Level 3 protocol would detect his attack, again, it is almost impossible to implement such a thorough security analysis. (FOF ¶ 1186.)

3. Dr. Johnston Performed His Attacks As Demonstrations. But He Is Not A Practiced Attacker; Therefore, The Court Should Not Take His Timings As Definitive.

The time that Dr. Johnston took to perform each attack does not represent the time that a real attacker would take. (FOF ¶ 1187.) Dr. Johnston readily admits that he is not skilled with his hands. (FOF ¶ 1187.) His expertise is in devising attacks, not in practicing them to perfection. (FOF

¶ 1187.) Dr. Johnston testified that an attacker with more agile hands would defeat New Jersey's proposed seals in a fraction of the time that it took him. (FOF ¶ 1187.) Beyond manual dexterity, however, no special qualifications are needed: Dr. Johnston testified that his Vulnerability Assessment Team has had artists practice attacks, because of their skilled hands. (FOF ¶ 1187.)

Further, Dr. Johnston has not had as much practice attacking the proposed seals as a real attacker would. (FOF ¶ 1188.) For example, Dr. Johnston practiced his attack on the Brooks Red Adhesive Tape Seal only 13 times. (FOF ¶ 1188.) Dr. Johnston testified that real attacker would practice an attack hundreds of times. (FOF ¶ 1188.)

Indeed, according to Dr. Johnston, the Vulnerability Assessment Team at Argonne does not focus on practicing attacks to perfection. (FOF ¶ 1189.) Instead, Dr. Johnston's team practices each attack just enough to show that it is a concern, so as to leave time for analyzing a broader range of attacks. (FOF ¶ 1189.) Dr. Johnston reported that an attacker, without the same overhead costs and tight schedule as Argonne, could spend as much time as she needs to perfect an attack. (FOF ¶ 1189.)

Again, Dr. Johnston testified that it is crucial to take every conceivable attack seriously, whether or not it has been demonstrated to perfection. (FOF ¶ 1190.) Dr. Johnston performed his attacks as a proof of concept, without the benefit of manual dexterity or hours of practice, but was nonetheless able to defeat every seal proposed for New Jersey's DREs. (FOF ¶ 1190.) A real attacker would be able to defeat the seals and install a fraudulent vote-stealing program even faster. (FOF ¶ 1190.)

4. Dr. Johnston Has Successfully Altered Election Results By Attacking The DRE Voter Panel, Circumventing The State's Proposed Seals Altogether. (This Section Discusses Dr. Johnston's Proffered Testimony.)

Dr. Johnston testified that the easiest way to defeat a seal is to go around it. (FOF ¶ 1191.)

New Jersey's DREs have no security features protecting the panel on which voters actually enter their votes, allowing an attacker to bypass all nine seals proposed by the State. (FOF ¶ 1191.) The voter panel comprises twelve identical subpanels, with buttons for voters to cast their votes. (FOF ¶ 1191.)

The subpanels are available to purchase, or can be taken from an unsecured voting machine in the warehouse. (FOF ¶ 1192.) Dr. Johnston has devised three successful attacks on the voter panels, which are described in his expert reports. (FOF ¶ 1192.) Dr. Johnston also made a proffer to the Court explaining that he was prepared to demonstrate the attacks on the record, and explaining some details of the attacks. (FOF ¶ 1192.)

The most devastating attack on the voter panel is what Dr. Johnston terms the "On/Off Attack." (FOF ¶ 1193.)

- Dr. Johnston is able to install a remote-control device on a subpanel, controllable from two hundred feet away, even through walls. (FOF ¶ 1193.)
- When the device is activated, it alters the subpanel circuitry so that all votes cast are directed to one candidate, without altering the behavior of the subpanel: a voter who pushes the button to vote for Candidate A will see a light indicating that her vote has been tallied for Candidate A, but the machine will record a vote for Candidate B. (FOF ¶ 1193.)
- When the remote-control device is switched off, the subpanel operates correctly, recording all votes as cast. (FOF ¶ 1193.)

An attacker is able to activate the device during voting to steal votes, and then turn it off at the end of the day so that the subpanel behaves correctly under testing; all he has to do is press a button on a pocket-sized transmitter. (FOF ¶ 1194.)

The total cost of this attack was $55, using equipment commonly used by hobbyists. (FOF ¶ 1195.) Dr. Johnston's expert opinion is that a high-school-age hobbyist could successfully effectuate the "On/Off Attack." (FOF ¶ 1195.)

Dr. Johnston was able to steal votes more simply by altering the wiring in the subpanels to swap votes. (FOF ¶ 1196.) The subpanel swap takes about twenty seconds, and in Dr. Johnston's opinion, can be performed by a twelve-year-old child. (FOF ¶ 1196.) A practiced attacker could even modify the subpanel circuitry while behind the voting booth curtain in one or two minutes. (FOF ¶ 1197.)

Dr. Johnston was able to install fraudulent subpanels in a DRE that was switched on and in voting mode without any problem. (FOF ¶ 1198.) Once the fraudulent subpanel is installed, an attacker can modify the removed subpanel and install it in a new machine. (FOF ¶ 1198.) That way, an attacker need only acquire one subpanel to attack a series of machines. (FOF ¶ 1189.)

The simplest attack of all on the voting panel is to replace the ballot sheet with a forgery that switches one or more columns, so that the column marked "Candidate A" actually records votes for Candidate B. (FOF ¶ 1199.) The result is that a district likely to vote for Candidate A actually goes to Candidate B. New Jersey publicizes the position of each candidate on the ballot sheet well in advance of the election. (FOF ¶ 1199.) An attacker can easily roll up a counterfeit ballot sheet and smuggle it into the booth hidden in the leg of his pants. (FOF ¶ 1199.) A second attacker can reinstall a normal ballot sheet at the end of the election to avoid detection. (FOF ¶ 1199.) This attack takes less than thirty seconds by removing a few normal screws; there are no security features in place to prevent the swap. (FOF ¶ 1199.)

Any of these voter panel attacks exploit Dr. Johnston's basic insight, that avoiding security seals is the best way to defeat them. (FOF ¶ 1200.) Given these design flaws in the DRE, seals cannot provide effective protection. (FOF ¶ 1200.)

D. IMPLEMENTING AN EFFECTIVE SECURITY PROGRAM BASED ON NEW JERSEY'S PROPOSED TAMPER-INDICATING SEALS WOULD INVOLVE GREAT TIME AND EXPENSE.

1. The State's Proposed Seals Will Not Provide Effective Security Without Detailed Use Protocols, Which Will Be Time-Consuming And Expensive To Develop.

Dr. Johnston testified that developing an adequate seal use protocol will take at least several months per seal. (FOF ¶ 1201.)

New Jersey has proposed six different kinds of seals for use in nine locations on its DREs. (FOF ¶ 1202.) It will take at least six months, possibly up to eighteen months, to lay the basic groundwork necessary for such a program to be effective. (FOF ¶ 1202.)

Dr. Johnston estimated that developing a seal use protocol would cost between $50,000 and $300,000 per seal, or between $300,000 and $1.8 million, at the outset, just to establish the basic protocols. (FOF ¶ 1203.)

2. In Order To Provide Effective Security, The State's Proposed Seals Would Require Detailed Inspections And Training, At Great Cost To The Taxpayers.

Dr. Johnston testified that conducting effective seal inspections would cost the state approximately an additional $492,000 per election, on top of the up to $1.8 million it will need to spend on developing basic seal use protocols. (FOF ¶ 1204.) He testified about the basis for this conclusion:

- Removing and inspecting the seals (including checking the serial numbers), removing the screws on the sheet metal covers, interior electronics inspection, reinstalling the sheet metal covers, reinstalling the seals, and recording the new seal serial numbers seals: 12 minutes. (FOF ¶ 1204.)
- Inspecting each of the 12 (subpanel) printed circuit boards inside the voters panel to look for modifications and alien electronics: 13 minutes. (FOF ¶ 1204.)
- Inspecting top, sides, and bottom of each DRE for damage: 4 minutes. (FOF ¶ 1204.)

- Additional time needed for dealing with Gorilla Glued seals, installing Red Tape Seals, and cleaning up adhesives: 15 minutes. (FOF ¶ 1204.)
- Total: 44 minutes.

At 44 minutes per DRE, 11,000 DREs would take roughly 8,000 person-hours to inspect.10 Dr. Johnston estimated the hourly cost of seal inspectors at $50, a conservative estimate. (FOF ¶ 1205.) The hourly cost of inspections may well exceed $50. (FOF ¶ 1206.) Technicians at federal facilities typically cost between $80 and $200. (FOF ¶ 1206.) A higher hourly rate, of course, yields a higher estimate of the overall cost of inspections. (FOF ¶ 1206.)

It is also necessary to train inspectors regularly, further inflating the cost of seal-based security. Dr. Johnston testified that inspectors must receive approximately 12 hours of hands-on training per seal. (FOF ¶ 1207.) To remain effective, the training must be repeated annually. (FOF ¶ 1207.)

With six kinds of seals in nine locations, New Jersey would have to devote at least seventy-two hours of training each year for every seal inspector on its payroll. (FOF ¶ 1208.) Furthermore, since maintenance staff would have to navigate the proposed seals in order to access batteries and circuitry, they would also need to be trained to remove, inspect, and reinstall all nine seals. (FOF ¶ 1208.)

3. Retroactively Adding Security Products To An Insecurely Designed System Does Not Work; In Such Instances, Dr. Johnston And His Team Recommend Exploring Different Security Approaches.

Even if New Jersey could afford to implement its seal program properly, its DREs would not be secure from tampering. (FOF ¶ 1209.) The fact is that no amount of retrofitting can remedy the inherent security flaws in New Jersey's proposed seals program. Dr. Johnston's expert opinion is

[10] This figure is based on Dr. Johnston's estimates in his original and supplemental expert reports.

that retrofitting a poorly designed system is never successful. (FOF ¶ 1209.) For a system to be secure, it must be designed securely, not modified as an afterthought. (FOF ¶ 1209.) Such efforts are not only costly, but futile in terms of security. (FOF ¶ 1209.) For that reason, Dr. Johnston's Vulnerability Assessment Team does not hesitate to recommend replacing an insecure system with one that is designed from the ground up with security in mind. (FOF ¶ 1209.)

Dr. Johnston testified that New Jersey's proposed security seals, even if properly implemented, cannot cure the engrained designed flaws in New Jersey's DREs. (FOF ¶ 1210.)

The State never introduced a single witness with any expertise in physical security. (FOF ¶ 1211.) The State had three months from the time Dr. Johnston filed his first report to the time he took the stand to call an expert in physical security to testify on its behalf[11], but failed to do so. (FOF ¶ 1211.) Dr. Johnston even recommended that the State consult a physical security expert in his report. (FOF ¶ 1211.) There is no testimony at all before this Court to refute Dr. Johnston; his expert conclusions remain uncotronverted. (FOF ¶ 1211.)

E. THE STATE HAS NOT PRESENTED ANY EVIDENCE THAT IT INTENDS TO SECURE WinEDS THROUGH HARDENING TECHNIQUES PROPOSED BY SEQUOIA. IN ANY RESPECT, HARDENING TECHNIQUES ARE IMPRACTICAL, EXPENSIVE AND LABOR INTENSIVE TO INSTALL AND MAINTAIN

1. The State has not Presented Any Evidence that it Intends to Use Hardening Techniques to Protect WinEDS

The State has not presented any evidence that it intends to use hardening techniques (such as reformatting the hard drives of WinEDS server and client computer networks or creating isolated networks) to protect the WinEDS system from viral attack. Only Mr. Smith addressed hardening methods, and he testified that he is aware that California and Nevada have sporadically employed

[11] Dr. Johnston's first report is dated February 2009. Johnston Expert Report, p. 35. He first took the stand on April 21 2009.

certain hardening techniques in the past, on a different voting machine, the Sequoia Edge. (FOF ¶ 881.) There is no other evidence in the record to indicate that the State has determined to use hardening techniques on the 11,000 DREs in New Jersey as a security measure.

2. Hardening Techniques are Impractical, Expensive and Labor Intensive

Plaintiffs' evidence, on the other hand, clearly demonstrates the impracticality of implementing the Sequoia hardening techniques.

One hardening technique recommended by Sequoia involves reformatting the hard drives of all of the computers in a county and then reinstalling clean copies of all of the necessary operating software, WinEDS software, and configuration information into each and every computer and server. (FOF ¶ 277.) Once the hard disk has been reformatted, clean copies of all the software and configuration information must be reinstalled on the hard drive. (FOF ¶ 279.) According to Mr. Smith, the reformatting/reinstallation procedure is automated and would take a medium-sized county of several hundred thousand voters approximately four hours to complete. (FOF ¶ 280.) Professor Appel testified that the reformatting procedures involve over 450 distinct steps that cannot be automated. (FOF ¶ 295.) According to Professor Appel's estimates, it would take several days to complete the necessary steps to reformat the hard drives and reinstall the software and configuration files. (FOF ¶ 295.)

The bulk of the Sequoia manual, "Sequoia Voting Systems Election Management System Reformatting and Reinstallation Guidelines," approximately eighty-eight pages, is dedicated to the explication of the reformatting and reinstallation hardening procedures. (FOF ¶ 281.) First, a master disk must be created by following the myriad steps in Chapters 2 through 4 of the Sequoia manual. (FOF ¶ 282.) This master disk is then applied to every single WinEDS client and server machine using the steps described in the Sequoia manual in Chapters 5, 6, 7, and 9. (FOF ¶ 282.)

The same master disk cannot be used from county to county because all counties do not uniformly have the same computer equipment running the WinEDS network. (FOF ¶ 284.) Creating the master disk depends in part on the particular county's network configuration, equipment, and the specific details of the local installation. (FOF ¶ 284.) Thus, one master disk will vary from another depending the county's equipment and installation details. (FOF ¶ 284.) Moreover, a master disk may not be useable on all of the servers and client computers within a given county. (FOF ¶ 285.) If the client and server computers vary in their internal hardware configurations, which would happen if they were purchased at different times or from different vendors, then a single master disk may not work. (FOF ¶ 285.) In that case, multiple master disks would have to be created from scratch, each from the 332-step process, each taking approximately 27 hours. (FOF ¶ 285.)

The creation of the master disk is only the first step in the reformatting and reinstallation procedures. (FOF ¶ 287.) Even after completing the 332 steps necessary to create a master disk, the reformatting and reinstallation procedure involves an additional 127 distinct steps as explained in chapters 5, 6, 7, and 9 of the manual to harden the WinEDS system from viral infection. (FOF ¶ 288.)

The instructions contained in the Sequoia manual assume a sophisticated understanding of what certain terminology means and what the import of certain configuration decisions would be in order to successfully follow the instructions to create a secure system that works. (FOF ¶ 287.) The installation and administration of the hardening techniques require the efforts of someone with a significant amount of expertise in information systems administration. (FOF ¶ 282.) Even Sequoia "strongly recommend[s] that a member of the IS team or someone experienced in building servers be consulted prior to attempting a server rebuild." (FOF ¶ 287.)

The second hardening technique recommended by Sequoia, the isolated network option, is just as impractical. This method of protecting against viral contamination of the WinEDS system is costly and redundant. To be most effective, according to Sequoia, the use of isolated networks requires three separate servers and possibly up to three networks to administer the election functions. (FOF ¶ 301.) As described in the Sequoia manual, one isolated server and client work stations would be for the purpose of preparing ballots before an election. (FOF ¶ 302.) A second isolated server and client work stations would be for the purpose of tallying election results. (FOF ¶ 302.) A third isolated server would be kept as a back-up network that can be used for one of the other two purposes. (FOF ¶ 302.)

Sequoia recommends that these three servers be isolated from each other and from the Internet so that viruses cannot easily propagate from one function (preparing the ballot) to the other function (tallying the results.) (FOF ¶ 303.) To implement Sequoia's recommendation, however, would require counties to triple their cost by purchasing three entire networks. (FOF ¶ 303.)

3. Hardening Techniques are not Needed With Software Independent Systems

All of the costs and the time-consuming efforts to implement the Sequoia hardening guidelines are unnecessary in software independent voting systems. (FOF ¶ 306.) While it is sound practice to run a clean and secure network installation like that described in the Sequoia manual, it is also possible to trust the results of an election without having to undergo the time-consuming and cumbersome hardening procedures Sequoia recommends. (FOF ¶ 308.) A system that allows for software independence, as required by Title 19, provides the New Jersey electorate with confidence that the State's 11,000 Sequoia DREs operate without viral infection. (FOF ¶ 309.)

F. THE LACK OF STATE OVERSIGHT OF ELECTIONS OR STATE-WIDE PROCEDURES FOR POLL WORKERS MAKES MANIPULATING ELECTION RESULTS EASY

The State's lax election-related procedures allow insiders to manipulate election results. Indeed, Michael Shamos, the State's expert witness, testified unequivocally that in his opinion insiders pose the greatest threat to election security. (FOF ¶ 1018.) Robert Giles testified that there are no State-wide election-related procedures for handling printed results reports and results cartridges after elections. (FOF ¶¶ 718-719.) He also testified that throughout the State results cartridges are used to tabulate official election results. (FOF ¶ 721.) This lack of standardized policy in handling election results leaves the results vulnerable to attack.

1. Paper Results Reports Printed at the Close of Polls are the Superior Form of Vote Tabulation.

When poll workers close the polls, a printer in the back of the Sequoia 9.00H DRE "automatically starts printing out a paper results report. (FOF ¶ 383.) The result reports are made by DREs (Pl. Exh. 25) "immediately when the polls close, in the presence of witnesses, [and are] signed by those witnesses[.]" (FOF ¶ 384.) The paper results report printouts come from the vote totals in the internal memory of the DRE. (FOF ¶ 384.)12

Professor Appel demonstrated on the video shown in Court (Pl. Ex. 6) how election results are printed on paper results reports, including where the results report shows that votes cast for Bill Richardson were attributed without detection to Dennis Kucinich by Professor Appel's fraudulent software (Pl. Ex. 21.) (FOF ¶ 87(c), 88.) There is space on the paper printout for "poll workers to sign on the lines that they witnessed that this is the paper that came out of th[e] machine." (FOF

[12] While votes are being recorded, the results report printer is inactive. (Appel, Tr., 01/27, 171:12-22.) Results reports contain information about the polling place, and are "supposed to be a record of how many votes have ever been cast on [the] machine[.]" (Appel, Tr., 01/27, 203:25-204:6.) The results report should also "print the public counter, which is how many voters have used th[e] machine in this election[]." (Appel, Tr., 01/27, 204:11-13.)

¶ 385.)

Even though the paper results reports printed when the polls close may reflect data manipulated by fraudulent firmware installed on a DRE (FOF ¶ 394), election results recorded on results cartridges can be manipulated much more easily. Due to this risk, results reports are superior to results cartridges as a source of election data. (FOF ¶ 397.) Dr. Shamos testified similarly, noting it is safer to rely on signed, authenticated results reports as the official election results. (Shamos, Tr., 03/24, 130:11-131:7.)

2. It is Easy for a Dishonest Poll worker or Election Staffer to Print Fraudulent Results Reports from Results Cartridges.

A results cartridge is a data cartridge about the size of a VHS tape. (FOF ¶ 568.) Results cartridges are inserted into each DRE prior to an election (FOF ¶ 224), and then inserted into cartridge readers on election night to tabulate votes. (FOF ¶ 573.)

The first vulnerability associated with results cartridges is that a dishonest poll worker can reinsert a fraudulently doctored results cartridge into the voting machine to print phony results reports. (FOF ¶ 386.) Other poll workers may not notice if a dishonest poll worker switched a legitimate results report for a phony results report. (FOF ¶¶ 386-388.)

Indeed, in Middlesex County the poll worker manual "explicitly recommends that poll workers perform other tasks at the very time the results report is printing[.]" (FOF ¶ 387.) Additionally, Professor Appel testified to seeing Mercer County poll workers casual treatment of results cartridges while they finish the paperwork required for closing the polls. (FOF ¶ 388.)

Plaintiffs did not have access to other poll worker manuals, as Defendants did not produce them in discovery. Thus, Plaintiffs could not demonstrate that the lax Middlesex and Mercer County practices are common. (See Appel, Tr., 01/27, 101:11-25, 156:9-15.) But, there is evidence those casual practices may indeed be prevalent. Robert Giles testified that there is no uniform, statewide procedure for protecting, handling, storing, or transporting results cartridges. (FOF ¶ 720.)

As such, while other poll workers are distracted, a dishonest poll worker can insert a phony results cartridge to produce a fake results report only minutes after the polls close. (FOF ¶¶ 386-388.)

3. Counties Rely on Results Cartridges for Official Election Results, and Do Not Use the Printed Results Report That is Signed by Witnesses When the Polls Close.

Robert Giles, the Director of the Division of Elections, testified that "throughout the State of New Jersey results cartridges are used to determine the vote totals at the end of each election." (FOF ¶ 721.)

This is confirmed by the testimony of both Joanne Rajoppi of Union County (FOF ¶¶ 614-615, 621; Rajoppi Test., 02/26 Trial Tr. at 50:8-11; 51:1-3; 52:2-8) and Paula Sollami-Covello of Mercer County. (FOF ¶¶ 573, 579-580.) County clerks use results cartridges to determine vote totals even though paper results reports are superior to results cartridges. (FOF ¶¶ 228, 394.)

After the election, results cartridges transmit election results to WinEDS computers at municipal or county locations. (FOF ¶¶ 388-389, 391.) WinEDs is the computer software that converts data on results cartridges into summary reports, which are printable. (FOF ¶¶ 41, 93, 202, 289, 618.) The summary results can be communicated within counties by email over the Internet. (FOF ¶¶ 615-617, 722.)

Election results are then posted to county websites within an hour or two on election night based on tabulation results gleaned from results cartridges that are used to electronically tabulate vote totals. (FOF ¶¶ 389, 579, 615-617; Rajoppi Test., 02/26 Trial Tr. at 42:1-21; 42:8-18; 43:3-16, 20-24; 50:8-11; 51:1-22; 52:2-8.) County clerks thereafter certify the election. (FOF ¶¶ 570, 581, 614, 621, 624.)

This testimony of Robert Giles and several county election officials directly contradicts the testimony and report of Dr. Shamos, the State's expert witness. Dr. Shamos asserts that "the 'use' of electronic totals by county clerks is for unofficial purposes on only[.]" (Shamos Report, ¶144; Shamos, Tr., 03/25, 33:3-17.) Many witnesses testified that this is not the case in New Jersey. Additionally, Dr. Shamos is incorrect that it is a "common misconception" that "the tabulation function performed by WinEDS on election night can determine the outcome of the election." (Shamos Report, ¶104, ¶143.) The State and county officials' testimony cited above makes clear that the results cartridges and not the results tapes determine the official election results.13 This was demonstrated clearly in 2008 in Camden County, where the County Clerk:

> used the data from the [results] cartridge in tabulating the election, even though this data disagreed with the data on the paper tape printout, and even though election technicians in Camden County had already logged information that could [be] easily interpret[ed] to mean the cartridge might not reliably contain the votes.

(FOF ¶¶ 355, 396, Appel, Tr., 02/04, 53:2-12; Appel Report, §57.14-57.17, Fig. 36.).)

4. The State Relies on Results Cartridges for Election Results Even Though There are Many Opportunities to Manipulate Results Cartridges.

Robert Giles testified that there is no uniform, statewide policy or procedure governing poll worker treatment of voting machines or their components. (FOF ¶¶ 713, 715-716, 719.) Mr. Giles also testified that "there [is] no uniform statewide procedure for transporting the cartridges from the polling sites to various county clerk's offices." (FOF ¶ 720.) Further, Mr. Giles admits the policies for transporting results cartridges differ from county to county. (FOF ¶ 720; Giles Test., 03/03 Trial Tr., 157:14-16.)

Results cartridges are <u>very</u> vulnerable to tampering and are easy to physically and

[13] The results are "unofficial" because they have not been added to absentee and provisional results, and the election has not been certified, (FOF ¶¶ 579, 581, 614, 621-624), not because the results tape is used as the official results in the

electronically manipulate even while they store election data. (FOF ¶ 391.) Neither hardware nor cryptography protects the data in the cartridge. (FOF ¶ 310; Appel Report, § 40.2, § 40.7, § 39; Shamos Test, 03/24 Trial Tr., 128:15-129:5.) When results cartridges are removed from DREs, they are immediately susceptible to manipulation. (FOF ¶ 391) (emphasis in original.) Because there is no uniform, statewide policy protecting the transportation of results reports and results cartridges (FOF ¶¶ 713, 715-716, 719), dishonest poll workers or election officials have ample opportunities to write fraudulent data to results cartridges. (FOF ¶ 390.)

A dishonest poll worker could use a simple program run from a personal computer to change votes on both the candidate total files and ballot image files. (FOF ¶¶ 390-393; see also Shamos, Tr., 03/24, 128:15-129:5.) Professor Appel's expert report also explains the ease of fitting a vote-stealing computer program onto a very small computer. This computer is smaller than a pack of cigarettes (FOF ¶ 393; Appel Report, §40.4-40.5, at Fig. 27-28) and can then be plugged into a results cartridge to quickly and surreptitiously change vote totals. (FOF ¶¶ 390, 392-393; Appel Report, §40.5.)

5. Results Cartridges Can Easily Be Acquired and be Converted, Falsified, or Altered to Manipulate Election Results.

Legitimate results cartridges can be altered to modify election results. Professor Appel reported that there are several simple, inexpensive ways results cartridges can be physically or mechanically altered to change election results. For example, official results cartridges can be physically altered to act differently[14] (Appel Report, §44-46), include readable and writeable

election.

[14] The list of vulnerabilities discussed here is not exclusive. Professor Appel explained that other data cartridges which "have the same size, shape, and appearance" (Appel Report, §44.1-44.2) as results cartridges, and can easily be rewired (Appel Report, §44.2, §46.3) to fraudulently steal votes at the polling place. (Appel Report, §46.3; 4.15, Fig. 5; §46.4, n. 89, §40.4-40.5, at Fig. 27-28.) Further, Professor Appel explained in his expert report that New Jersey should not use early voting cartridges on AVC Advantage DREs. (Appel Report, §45.) Further, the risk presented by consolidation

memory (Appel Report, §47), or steal votes. (Appel Report, §48.) It is not difficult to acquire results cartridges and make these alterations. As Professor Appel testified, he bought five Sequoia Advantage DREs and five result cartridges on the Internet for $82. (FOF ¶ 130; Appel Report, §11.6-11.7.)

Additionally, election workers and outside vendors can steal cartridges from the counties. Mr. Giles testified that there is no uniform, statewide policy regarding how results cartridges are stored by counties. (FOF ¶ 719.) They are not secured in any meaningful way. Elisa Gentile testified that in Hudson County all five-hundred cartridges are stored "in the open" on a wheeled casing. (Gentile, Tr., 02/23, 54:16-25, 55:23-13.) Additionally, after results cartridges are loaded into DREs at the warehouse (FOF ¶ 484; Gentile, Tr., 02/23, 47:17-25, 48:1-3, 50:25-51:19, 75:1-4), a vendor may access hundreds of DREs over several days without county supervision. (FOF ¶ 484; Gentile, Tr., 02/23, 48:2-50:18.)

Similarly, Daryl Mahoney testified that Bergen County's results cartridges are stored in lockable cabinets in a computer room at the county voting machine warehouse (FOF ¶ 527), stacked and labeled by town. (FOF ¶¶ 521, 527; Mahoney, Tr., 02/23, 117:2-118:10.) Paula Sollami-Covello testified that results cartridges in her county are also stored at a county warehouse. (FOF ¶ 583.)

The cartridges are also often left unattended in open voting machines where both county workers and outside vendors can access them. Election mechanics are given unfettered access to DREs. (FOF ¶ 523; Mahoney, Tr., 02/23 99:17-100:21, 103:12-34, 118:2-14.) When Bergen County upgraded the DRE software, outside vendors were given unfettered access to the machines for several weeks. (FOF ¶ 530.)

cartridges, for example, is "very dangerous" because the pre-election vote doctoring can easily go undetected. (Appel

Professor Appel also explained that it is "very easy" and requires "very little technical skill" to make fake results cartridges (Appel Report, §47.11) to include an inexpensive,15 wirelessly-enabled, radio-controlled flash memory card. (See Appel Report, §47.5, 47.11.) Even a college student could "make a 'smart' results cartridge that fools the motherboard." (Appel Report, §48.1.) A "poll worker, election worker, . . . or a voter" could easily attack the cartridge wirelessly from several feet away (Appel Report, §47.7) to manipulate ballot data and election results while the cartridge is installed in DRE or after its removal. (Appel Report, §47.11, §48.3.)

It would not be easy for a poll worker or election official to detect fraudulent cartridges, which "have the same appearance as ordinary cartridges" (Appel Report, §48.5) and would be designed with a computer program inside (Appel Report, §48.3, §48.6) to steal votes "in election after election" with no human intervention. (Appel Report, §48.6; see Appel Report, §6.15.)

Because there are no uniform, statewide policy or procedures for where counties count votes from cartridges (see FOF ¶¶ 718-719), results cartridges can be altered or replaced while they are being transported after the election. (See FOF ¶¶ 390-391.)

Mr. Giles testified that votes may be counted by municipal workers rather than by county workers. (See FOF ¶¶ 721-722; see Giles, Tr., 03/03, 157:10-16), and the Court acknowledged that results cartridges are sometimes brought to a municipal clerk, who sends data electronically to the county clerk. (See Shamos, Tr., 03/23, 156:7-157:6.)

In Union County, Joanne Rajoppi instituted procedures to protect election results. Results cartridges and reports are transported directly to municipal clerks (Rajoppi, Tr., 02/26, 45:17-22, 46:9-13, 131:12-19), whereafter sheriffs transport the cartridges to "satellite offices" to be read (FOF

Report, §40.4, 46.4; Appel, Tr., 01/29, 100:11-15.)

[15] Professor Appel cites, for example, a wirelessly enabled two gigabyte compact flash card sold for $49.99 under the brand name Eye-Fi, available at http://www.eye.fi. (last visited, June 15, 2009.)

¶¶ 615-617; Rajoppi, Tr., 02/26, 41:1-7, 44:2-45:14, 45:25-46:2) before they are stored with the county clerk. (FOF ¶ 615.) Ms. Rajoppi's "exemplary practice" of results cartridge security (Appel Report, §41.7), however, does not protect the cartridges immediately after they leave the polling place.

By contrast, in Mercer County, results cartridges are transported to municipal clerks offices, where county workers pick them up. (FOF ¶ 570.) Afterwards, every cartridge is read at the county clerk's office. (FOF ¶¶ 571-573.) James Clayton of Ocean County and Daryl Mahoney of Bergen County testified to similar practices in their counties. (Clayton, Tr., 03/03, 58:9-59:1-5; FOF ¶ 540.)

Thus, in Mercer, Ocean, and Bergen County, results cartridges can be manipulated by poll workers or municipal workers en route to the municipal clerk (FOF ¶¶ 310, 390-391) and by county workers en route to the county clerk. (See Clayton, Tr., 02/24, 58:17-24; Sollami-Covello, Tr., 02/24, 60:19-61:17; see Mahoney, Tr., 02/23, 122:7-123:18; FOF ¶¶ 310, 390-391.)

The State has not presented any witnesses to rebut Professor Appel's testimony about the insecure nature of results cartridges. Indeed, Dr. Shamos examined how cartridges could be manipulated after being removed from voting machines after the election, en route to the county clerk's office. (FOF ¶¶ 932, 940, 943, 950; Shamos, Tr., 03/23, 42:1-11; Shamos, Tr., 03/24, 128:15-129:5.)

The State also presented no testimony whatsoever to show there are safeguards in place which ensure election results recorded on results cartridges are protected against manipulation. Indeed, the State concedes that manipulation by insiders is a significant threat to election results. The State's expert witness, Dr. Shamos, testified that the principle threat security experts worry about is what insiders can do because insiders do not have to defeat the physical security. (FOF ¶ 950.) He also noted "[i]t is of course important to institute procedures to ensure that insiders cannot mount the attacks proposed, or to ensure that any intrusion will be detected." (FOF ¶ 950.)

6. The State Does Not Require That Signed, Printed Result Reports Be Compared Against Results Cartridge Results.

Robert Giles testified that he has not instituted a requirement that county clerks compare the results cartridge with paper results report printouts. (See FOF ¶¶ 721, 723.) Comparing paper results reports with cartridge results can detect changes made to election results in the results cartridge after the paper report is printed. (See FOF ¶¶ 394-395, 582, 621, 625; Appel Report, § 45.3.)

In sum, New Jersey counties rely on results cartridges for official election data, paying scant if no attention to the printed results tape produced by the DREs at the close of the polls, that are signed by witnesses. Uncontroverted evidence was presented at trial that election data stored on results cartridges is easy to manipulate. This evidence was not contradicted or rebutted by any defense witnesses. As defense expert Michael Shamos testified, poll workers and election workers have many opportunities to manipulate the data, and pose a real risk to election results.

Although vulnerable to tampering by the replacement of a DRE's firmware (FOF ¶¶ 74-75), printed results reports produced by DREs on election night are vulnerable to fewer kinds of fraudulent tampering than results cartridges. Thus, results reports are a more accurate source of election results. (FOF ¶ 394.)

Despite this, there is no statewide requirement that results reports be compared against cartridge data. (See FOF ¶¶ 718-719, 228, 394; see Appel, Tr., 01/28, 5:13-24; Appel Report, §41.4.) This is still the case, even though the 2008 Presidential primary, comparing results reports against cartridge data in eight counties demonstrated many inconsistencies between printed results reports and election results stored on results cartridges.

VII. THE COURT SHOULD GIVE GREATER CREDENCE TO PLAINTIFFS' EXPERTS' TESTIMONY BECAUSE THEY ARE BETTER QUALIFIED TO

ASSESS THE RELIABILITY AND ACCURACY OF THE SEQUOIA ADVANTAGE 9.00H AND BECAUSE, UNLIKE THE DEFENDANTS' WITNESSES, THEY ARE NOT BIASED

The trial judge, when serving as fact-finder, is well-positioned to evaluate the credibility and qualifications of an expert witness as well as the weight to be afforded to the expert's testimony. See In re Guardianship of DMH, 161 N.J. 365, 382 (1999); see also State v. Clark, 104 N.J. Super. 67, 75 (Law Div. 1968) (judge sitting as trier of fact determines weight to which expert testimony is entitled and may choose to reject an expert's opinion.) Factors relevant to assessing an expert's credibility include the expert's background, training, experience, familiarity with the circumstances of the case, rationality and consistency of testimony, and any motives, bias, or interests that could have influenced the expert's opinion. See Rubanick v. Witco Chem. Corp., 125 N.J. 421, 453 (1991) (quoting Wells v. Ortho Pharmaceutical Corp., 615 F. Supp. 262, 266-67 (N.D. Ga. 1985).)

Plaintiffs respectfully submit that this Court should afford greater weight and credence to the testimony of Plaintiffs' experts. As explained in further detail below, Plaintiffs' experts possess qualifications superior to those of Defendants' experts, and have specific knowledge of the Sequoia Advantage 9.00H DREs and security seals. Further, unlike Defendants' experts, Plaintiffs' experts presented opinions and beliefs that are shared by members of the scientific community, and have no personal interests or biases related to this litigation.

A. PLAINTIFFS' EXPERTS ARE BETTER QUALIFIED

An expert's qualifications and experience are highly relevant to evaluating the credibility of the expert's testimony. See Interfaith Cmty Org. v. Honeywell Int'l, Inc., 263 F. Supp. 2d 796, 805-12 (D.N.J. 2003) (giving substantial consideration to educational background, knowledge, and relevant experience of expert witnesses in assessing weight to afford their testimony); Thermographic Diagnostics, Inc. v. Allstate Ins. Co., 125 N.J. 491, 497 (1991) (finding expert testimony unpersuasive where experts "lacked the research and scientific credentials that would have imparted greater weight and credibility to their opinions".) Plaintiffs' experts – Professor Andrew Appel, Dr. Roger Johnston, and Professor Wayne Wolf – possess outstanding credentials, knowledge, and experience, making them substantially better qualified to assess the reliability, accuracy, and security of the Sequoia Advantage 9.00H than Defendants' experts.

1. Professor Andrew Appel

Professor Appel is an extraordinarily qualified witness in the areas of computer science, computer security, the Sequoia Advantage DRE, and the WinEDS system. He received a bachelor's degree in physics with highest honors from Princeton University in 1981, specializing his undergraduate work in applications of computer science to physics. (FOF ¶ 16.) He proceeded to earn a Ph.D. in computer science from Carnegie Mellon University in 1985, focusing his Ph.D. research in methods of reasoning to ensure the correctness and accuracy of computer software. (FOF ¶ 17.)

Professor Appel's employment history also makes him uniquely qualified to render an opinion in this case. Professor Appel served as a computer science consultant for Bell Laboratories for many years. (FOF ¶ 18.) He has been a professor of computer science at Princeton University since 1986, tenured since 1992, and a full professor at Princeton since 1995. (FOF ¶ 15.) Professor Appel teaches courses in software engineering, programming languages, compilers, and election machinery - a course that involves not only voting machines, but also political party machines, and the machinery of election administration by public officials. (FOF ¶ 21.) He also teaches computer security in the context of software engineering courses at the sophomore level, and supervises and advises graduate students who conduct computer security research. (FOF ¶ 24.) In addition to teaching, Professor Appel has an appointment to the Center for Information Technology Policy at

Princeton, an interdisciplinary center that studies the intersection between computer science and public policy. (FOF ¶ 19.) Professor Appel served as Associate Chair of the Department of Computer Science at Princeton University for approximately ten years between 1996 and 2005, and will become the next Chair of the Computer Science Department. (FOF ¶ 20.)

Professor Appel has been conducting computer science research since 1980, and researching computer security in particular since 1994. (FOF ¶ 16.) His extensive scientific research ranges from theoretical aspects of computer security that overlap with programming languages and formal methods, to practical computer security topics, such as securing enterprise computer networks, physical security, and security of computer memory systems, among others. (FOF ¶ 25.)

Professor Appel has continuously been awarded research grants for his professional work, including a grant from the National Science Foundation for research in programming languages, compilers, and computer security. (FOF ¶ 23.) He has also received research grants from the Defense Advanced Research Projects Agency for research in computer security, and from the Advanced Research and Development Activity, a funding agency within the United States Intelligence Community. (FOF ¶ 23.) He recently received a grant for research in computer security from the Air Force Office of Scientific Research. (FOF ¶ 23.) In addition to grants from government agencies, Professor Appel has also received research grants from many corporations, such as IBM, Microsoft, and Sun Microsystems. (FOF ¶ 23.)

Professor Appel has earned numerous accolades and appointments in the computer science field. Since 1998, he has been an honorary Fellow in the Association for Computing Machinery, an international professional society of computer scientists, both in academia and industry, with tens of thousands of members. (FOF ¶ 22.) Professor Appel has also served as a member of the program committee, or a chair of the program committee, of several different conferences on computer science, which included topics such as programming languages, compilers, logic, and voting machines. (FOF ¶ 28.) He has been an associate editor of two journals, and has served as editor-in-chief for the Association for Computing Machinery's journal, during which time he supervised hundreds of papers through the publication process, including papers on computer security. (FOF ¶ 27.) Professor Appel's curriculum vitae enumerates ninety publications, of which eighty-three, including two books and a chapter of another book, were published in peer reviewed venues. (FOF ¶ 26.)

Professor Appel was certified by this Court as an expert in computer science and computer security, as well as an expert on the Sequoia AVC Advantage DRE that is the subject of this trial. (FOF ¶ 45.) Defendants called no witness to rebut the scientific testimony of Professor Appel. His conclusions that New Jersey's DREs are unreliable and insecure are uncontested.

2. Dr. Roger Johnston

Plaintiffs' second expert, Dr. Roger Johnston, is one of the world's leading experts regarding issues of physical security and security culture, and thus was highly qualified to provide testimony about the poor physical security of New Jersey's DREs. Dr. Johnston earned both an MA and Ph.D. in physics from the University of Colorado in 1983. (FOF ¶ 1061.) He is employed as a Senior Systems Engineer at Argonne National Laboratories, a federal laboratory owned by the Department of Energy and run by the University of Chicago. (FOF ¶ 1061.) Dr. Johnston is Section Manager of Argonne's Vulnerability Assessment Team, which examines security devices, systems and programs, identifies flaws, and recommends countermeasures. (FOF ¶ 1062.) His team at Argonne works on projects with sensitive national security implications, including nuclear safeguards and security applications. (FOF ¶ 1062.) Dr. Johnston's work has made him one of the world's preeminent experts on security. (FOF ¶ 1029.) In fact, Ross Anderson, Professor of Security

Research at Cambridge University, has written that "the most impressive physical security research team in the world is probably Roger Johnston's Vulnerability Assessment Team." (FOF ¶ 1068.)

Before working at Argonne, Dr. Johnston founded the Los Alamos National Laboratories Vulnerability Assessment Team, and spent fifteen years as its Team Leader.[16] (FOF ¶ 1065.) There, Dr. Johnston worked on projects involving homeland security, nuclear safeguards and nonproliferation compliance, counter-terrorism, biophysics, chemistry, and laser applications, in addition to security seals and tamper detection. (FOF ¶ 1065.) He has also consulted for the Department of Energy, the Department of Defense, the Nuclear Regulatory Commission, the National Institutes of Health, and numerous private corporations. (FOF ¶ 1065.)

Over the past twenty years, Dr. Johnston has studied hundreds of kinds of security seals, and published over 115 articles on seals and security. (FOF ¶ 1064 .) He is Editor of the Journal of Physical Security, and holds a U.S. government Top Secret Q clearance, allowing him to study seals used on nuclear safeguards and other sensitive national-security applications. (FOF ¶ 1064.) Dr. Johnston has won numerous awards and fellowships, including several research and achievement awards at Los Alamos, and a Distinguished Performance Award from the Central Intelligence Agency in 2002. (FOF ¶ 1066.) From 2001-2002, he was a Science Fellow at the Center for International Security and Cooperation at Stanford University. (FOF ¶ 1067.)

In its Rule 104 Hearing of April 21, the Court certified Dr. Johnston to give expert testimony on everything covered by the expert report he submitted, along with its addendum. (FOF ¶ 1071.) Under the Court's certification, Dr. Johnston's expertise covered all aspects of physical security, including security seals, security culture, physical vulnerabilities, attacks on seals, inspections, backdoor attacks, DRE storage, and background checks. (FOF ¶ 1071.) Defendants did not call any

[16] Los Alamos, like Argonne, is a federal national laboratory owned by the Department of Energy. (FOF ¶ 1065.)

witnesses with expertise in physical security. Thus, Dr. Johnston's testimony is the only testimony before the Court on the subject of physical security as it relates to New Jersey's DREs. (FOF ¶ 1072.) His conclusions – that New Jersey has no security culture, and that the Defendants' proposed seals can be defeated without detection – are uncontested by any expert or evidence. (FOF ¶ 1072.)

3. Professor Wayne Wolf

Plaintiffs' third expert, Professor Wayne Wolf, possesses outstanding credentials and qualifications in the field of processor design and embedded security. Professor Wolf serves as Professor Rhesa, Ray. S. Farmer, Jr., Distinguished Chair of Embedded Computing Systems and Georgia Research Alliance Eminent Scholar at Georgia Institute of Technology. (FOF ¶ 1212.) He received his Bachelor's degree, Master's degree, and Ph.D. in Electrical Engineering from Stanford University. Following the receipt of his Ph.D. in 1984, Professor Wolf accepted a position as Professor at Princeton University and subsequently joined the faculty at the Georgia Institute of Technology in 2007. (FOF ¶ 1213.) He has also held several industry positions since receiving his Ph.D., including consulting for several companies and holding leadership titles at MediaWorks Technology in 2001 and 2002. (5/11 Trial Tr. at 8:24 to 9:5.) He currently holds the positions of director, secretary, and vice-president at Verificon Corporation. (5/11 Trial Tr. at 9:3-5.)

Professor Wolf has been involved with several notable and relevant publications. He was the founding editor-in-chief of the journal for the Association for Computing Machinery ("ACM"), TRANSACTIONS ON EMBEDDED COMPUTER SYSTEMS. (FOF ¶ 1214.) He also served as editor-in-chief of the Institute of Electrical and Electronics Engineers ("IEEE") journal, TRANSACTIONS ON VSLI SYSTEMS. (FOF ¶ 1214.) Professor Wolf has authored four major textbooks, including texts on VSLI ("Very Large Scale Integration"), FPGA-based system design, and embedded computing. (FOF ¶ 1214.) He has conducted extensive research on microprocessors and has taught classes on microprocessors and embedded computing at Princeton and Georgia Tech. (5/11 Trial Tr. at 9:5-23; 12:4 to 14:4.)

Further, Professor Wolf has received many distinguished awards for his work on computer systems, including the Frederick E. Terman Award from the American Society for Engineering Education. (FOF ¶ 1215.) He has also been named a Fellow of both the IEEE and the ACM. (FOF ¶ 1215.)

Professor Wolf was certified as an expert in microprocessors, including embedded computing, logic design, and VLSI design. (FOF ¶ 1216.) He was also certified as an expert in embedded system security. (FOF ¶ 1216.)

B. DEFENDANTS' EXPERTS ARE NOT QUALIFIED TO ISSUE OPINIONS CONCERNING NEW JERSEY'S DREs

The qualifications, backgrounds, and experiences of Plaintiffs' experts are far superior to those of Defendants' three expert witnesses, who lack the necessary qualifications to render their opinions credible. See Thermographic Diagnostics, Inc, 125 N.J. at 497.

Defendants' first expert, Dr. Michael Shamos, lacks qualifications as a computer security expert. While Dr. Shamos may have a Ph.D. in computer science, he has a very thin publication history, and those publications are not particularly germane to any matters related to this case. (FOF ¶ 898.) His published articles ranging in topics from the piezoelectric effect in bone to mathematics, intellectual property law, worker's compensation, and academic titles. Conspicuously absent from this extensive list is a single publication about computer security. (FOF ¶ 898.) Further, although Dr. Shamos lists five books on his resume, four of them are different translations of the same book - a textbook on computational geometry, a field generally associated with computer graphics - and the other book is merely a directory of academic titles used at Carnegie Mellon University. (FOF ¶ 899.) Dr. Shamos does have some sparse writings on the subject of voting, but he concedes that these are mostly about the history of voting, rather than current practice. (FOF ¶ 900.) He has written no books on computer security or voting, and his papers about voting mostly consist of papers delivered at conferences, not peer reviewed publications. (FOF ¶ 900.)

Moreover, despite a thirty-four year affiliation with Carnegie Mellon University, Dr. Shamos is only adjunct faculty and is not a tenured professor at the institution. (FOF ¶ 901.) During most of his affiliation with the University, he has not been engaged in scientific research in the field of computer science, but has instead practiced law and written dozens of articles and books on billiards. (FOF ¶ 901.)

Unlike Professor Appel, Dr. Shamos does not advise any Ph.D. students, and has not received any recent awards in the field of computer science. (FOF ¶¶ 902-903.) The last awards Dr. Shamos won related to computer science are from twenty and thirty years ago; he has contributed little to the development of the rapidly evolving field since then. (FOF ¶ 903.) In fact, the only awards received by Dr. Shamos since that time have been in fields such as law, billiards, and bagpipes. (FOF ¶ 903.)

Defendants' remaining expert witnesses, Edwin Smith and Paul Terwilliger, are in fact employees of Sequoia. Prior to the commencement of trial, the Defendants never indicated any intent to call Mr. Smith and Mr. Terwilliger as expert witnesses in support of its case. (FOF ¶ 778.) On January 27, 2009, just before the start of trial, the Court ruled that the Defendants' identified expert, Dr. Shamos, would not be allowed "to testify as to whether in his opinion the voting machines are scientifically accurate or reliable." (FOF ¶ 779.) One week later, on February 4, 2009 at 6:04 p.m., four days into trial, and after being in Court with Plaintiffs' counsel all day, Plaintiffs' counsel received (via email) a letter from Ms. Gore stating that the "State defendants intend to call Sequoia representatives Ed Smith and Paul Terwilliger as experts in our case-in-chief." This was the very first time that Plaintiffs were notified in writing of the Defendants' intention to convert Mr. Smith and Mr. Terwilliger from fact witnesses to expert witnesses. (FOF ¶ 780.)

Not surprisingly, Mr. Smith and Mr. Terwilliger do not possess impressive credentials and qualifications for providing an expert opinion. For example, Mr. Smith holds degrees in mechanical engineering and business administration, not in computer science or computer engineering. (3/18 Trial Tr. at 59:23 to 61:10.) Likewise, Mr. Terwilliger does not hold any degrees in computer science or computer engineering, has never held any academic appointments or published any articles in peer-reviewed journals, and has had no professional speaking engagements other than sales-related presentations. (3/30 Trial Tr. at 24:25 to 26:7-24.) In addition to lacking the qualifications and background necessary to render credible expert opinions, Mr. Smith and Mr. Terwilliger, as employees of Sequoia, are heavily biased based on personal interests, as detailed in Subsection D, below.

In sum, the qualifications, educational backgrounds, and relevant experiences of Plaintiffs' experts far exceed those of Defendants' experts. Thus, Plaintiff's experts are better qualified to assess the reliability and accuracy of the Sequoia Advantage 9.00H, and their opinions should be afforded greater weight by this Court than the opinions of Defendants' experts.

C. PLAINTIFFS' EXPERTS EXAMINED THE DREs AND SECURITY SEALS

In addition to the paramount qualifications of Plaintiffs' experts, their testimony warrants greater credence because, unlike Defendants' experts, Plaintiffs' experts conducted a thorough physical examination of the Sequoia Advantage 9.00H DREs and security seals.

Professor Appel's personal study of Sequoia AVC Advantage 9.00H DREs provides a rock solid scientific foundation for his expert opinion. In connection with this lawsuit, in July and August 2008, Professor Appel and a team of computer scientists examined two Sequoia AVC Advantage

9.00H DREs voting machines provided by Defendants. (FOF ¶ 29.) Professor Appel and his team spent an extraordinary number of hours inspecting and experimenting on the Advantage 9.00H DREs. During the month of July 2008, the team spent almost seven days a week examining the DREs, working from six to ten hours a day. (FOF ¶ 31.) These examinations looked at a number of aspects of the DREs, including, but not limited to, source code, operation of the DREs, and how the WinEDS database computers interact with the DREs. (FOF ¶ 41.)

Following the thorough physical examination of the Sequoia 9.00H DREs, Professor Appel wrote a lengthy and detailed report containing narrative descriptions of the various insecurities and inaccuracies in the DREs that he was able to uncover during the thirty-day examination. (FOF ¶ 36.) In addition, on August 20 and 21, 2009, Professor Appel created a videotape demonstrating inaccuracies and insecurities in the Sequoia DREs. (FOF ¶ 42.)

Despite many limitations and difficulties imposed by Defendants on Professor Appel's experiments,[17] Professor Appel and his team were able to engage in much of the necessary examination of the DREs. (FOF ¶ 35.) They gave Professor Appel a solid scientific foundation for the conclusions he reached in his expert report; the statements he made on his videotaped demonstration about the unreliability, insecurity and inaccuracy of the Sequoia DREs; and the elaborately detailed and meticulously reasoned opinions he gave in his expert testimony before this Court. (FOF ¶ 35.)

[17] Defendants erected numerous obstacles to Plaintiffs' examination, depriving Professor Appel and his team of the opportunity to perform some tests and procedures they would otherwise have conducted. For example, despite repeated promises to replace defective daughterboards after they ceased functioning, Defendants never did so, depriving Plaintiffs of an opportunity to demonstrate numerous flaws in these components. (FOF ¶ 32; Exs. P-22A, P-22B, P-22C, P-22D, P-22E.) Further, despite having had months to prepare for the Court-ordered examination of the Sequoia DREs on June 30, 2008, Sequoia produced a grossly incomplete subset of the source code, which failed to include the source code for numerous third party library files, lacked build tools such as a compiler, and completely lacked any source code, firmware, or configuration files for the operating system on the daughterboard. (FOF ¶ 33.) If given the time, Professor Appel would have fabricated a fraudulent Z80 chip. (FOF ¶ 34.) This project would have taken Professor Appel at least a month, and possibly as long as three months. (FOF ¶ 34.)

Plaintiffs' experts have also examined the security seals introduced by the Defendants. Since becoming involved in this case in 2009, Dr. Johnston has examined no fewer than thirteen seals, all of which were introduced after discovery ended. (FOF ¶ 1075.) Dr. Johnston testified that in seventeen years at the forefront of his field, he has never seen so many seals used at once, including on top-secret nuclear safeguards and other high-level national-security applications. (FOF ¶ 1080.) He concluded that the unprecedented complexity of New Jersey's seals will overwhelm seal inspectors, as they struggle to do a good job on every seal under a more and more minutely detailed rubric. (FOF ¶ 1082.)

Further, during both direct and cross examination, Dr. Johnston demonstrated to the Court that simple, low-tech, inexpensive methods exist for defeating all of New Jersey's proposed seals. (FOF ¶ 1096.) In open court, he defeated all of the seals contemplated by the Defendants, despite the fact that the Defendants continued changing its proposed seals as late as April 2009. (FOF ¶ 1097.)

Moreover, Professor Appel, who is not a burglar, was also able to defeat all the seals introduced by the Defendants. (FOF ¶ 138.) Even when confronted in cross-examination and forced to perform his hacks on the spot, Professor Appel was able to break into the Sequoia Advantage 9.00H and replace the legitimate ROM chip with a fraudulent one. (FOF ¶ 138.)

Unlike Plaintiffs' experts, Defendants' experts did not base their opinions on a physical examination of the equipment at issue, but rather on personal opinion and the Sequoia company's beliefs. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the Defendants, Dr. Shamos never tested the Sequoia AVC Advantage 9.00H, and spent only one hour with the equipment. (FOF ¶¶ 919-920.) Dr. Shamos described his interaction with the DRE by saying that he merely "exercised the machine so that I could see the effect of the option switch bug." (FOF ¶

921.) Tellingly, Dr. Shamos did not examine or test the source code, firmware, or hardware of the AVC Advantage 9.00H, nor did he research the Defendants' proposed security seals. (FOF ¶¶ 922-924.)

Furthermore, both Mr. Terwilliger and Mr. Smith testified that they performed no tests, experiments, or measurements in connection with the assertions made in the Sequoia Response report. (FOF ¶¶ 818, 820.) Therefore, Plaintiffs' experts' opinions regarding the DREs and security seals merit greater credence than Defendants' experts' opinions, which were not based on an informed physical inspection of the equipment at issue in this litigation. See Suanez v. Egeland, 353 N.J. Super. 191, 196 (App. Div. 2002) (holding that opinion of defendant's expert lacked reliable foundation in part because expert did not personally conduct or observe tests of type of auto collision at issue.)

D. PLAINTIFFS' EXPERTS' OPINIONS AND BELIEFS ARE SHARED BY MEMBERS OF THE SCIENTIFIC COMMUNITY, WHILE DEFENDANTS' EXPERTS' OPINIONS ARE NOT

In determining the amount of credence to afford the testimony presented by the experts at trial, this Court should also consider the fact that the opinions and beliefs of Plaintiffs' experts are generally shared by the scientific community, whereas the opinions and beliefs of Defendants' experts are not. See Rubanick, 125 N.J. at 432 (reliability of expert testimony may be established by demonstrating general acceptance of expert's opinion or theory within scientific or professional community); Suanez, 353 N.J. Super. at 195 (scientific evidence must be "supported by some expert consensus".) Courts will generally afford diminished weight and credibility to expert testimony that is inconsistent with the views of other experts in the field. See Interfaith Cmty Org., 263 F. Supp. 2d at 812 (rejecting testimony of defendant's expert that was at odds with most or all of other experts.)

The views of Plaintiffs' experts are supported by the consensus of the scientific community.

Professor Appel testified that the consensus among experts in computer security who study voting systems is that software independence – verification of vote totals independently of the computer program used to count them – is the only reliable way of assuring security and accuracy in an election in which computers are used. (FOF ¶¶ 402-403.) Currently, the only commercially available technology which achieves software independence is the voter-verified paper ballot, either in the form of the precinct-based optical scanner or in the form of DREs that print a paper ballot. (FOF ¶ 404.)

Professor Appel testified as to the superiority of precinct-based optical-scan systems, and recommends that New Jersey adopt this technology. (FOF ¶¶ 423-433.) This view is shared by the overwhelming majority of computer scientists and election technology experts, who have concluded that precinct-based optical-scan systems are the most trustworthy, robust, and cost-effective method of voting currently available. (FOF ¶ 433.)

The opinions of Defendants' experts, in contrast, are not shared by members of the scientific community. Significantly, Dr. Shamos is the only expert who supports paperless voting systems that cannot be independently audited by paper ballots. When asked if he could identify any other computer scientists or computer security experts who agreed with his position that paperless DREs are superior to DREs that produce a voter-verified paper ballot, Dr. Shamos named just two individuals who might agree with this position. (FOF ¶¶ 926-927.) When further questioned about these individuals, however, Dr. Shamos admitted that they in fact supported software independence, precinct-based optical scanners, or a software independent voter-verified paper audit trail, not paperless DREs. (FOF ¶¶ 928-929.)

Moreover, the theoretical testing methods proposed by Dr. Shamos for detecting fraudulent software - parallel testing, checkpointing, and the Prime III Voting Machine –do not exist, as

Professor Shamos envisions them and have never been tested. (See generally FOF ¶¶ 1019-1051.) All computer security experts favor software independence and precinct-based optical scanners to Dr. Shamos's theoretical testing methods. (FOF ¶ 1019.) Thus, Dr. Shamos's opinion concerning paperless DREs should not be afforded credence by this Court. See Interfaith Cmty Org., 263 F. Supp. 2d at 812.

E. PLAINTIFFS' EXPERTS ARE NOT BIASED, WHILE DEFENDANTS' EXPERTS ARE BIASED

Each of Defendants' experts has a financial interest in the outcome of this case, severely calling into question the objectivity and credibility of their opinions. Courts routinely and properly afford diminished or no weight to the testimony of an expert who has an economic interest related to the parties or subject matter of the litigation. See, e.g., Thermographic Diagnostics, Inc., 125 N.J. at 497 (concluding that experts' financial interest in company that owned medical equipment at issue impaired objectivity of their testimony); Interfaith Cmty Org., 263 F. Supp. 2d at 812 (rejecting testimony of defendants' expert as "unfairly biased" where expert's primary source of income was his ongoing professional relationship with defendant.)

1. Defendants' Expert Smith's Personal Interest

Defendants' expert Edwin Smith has a compelling personal stake in the outcome of this litigation. Mr. Smith is a member of Sequoia's senior management team and has been Sequoia's vice-president of Compliance since May 2006. (FOF ¶ 781.) In addition to the salary he receives from Sequoia, Smith receives bonuses based on Sequoia's revenue and profit in a given year. (FOF ¶ 782.) Moreover, Mr. Smith has an ownership interest in Sequoia. (FOF ¶ 783.) According to Mr. Smith, Sequoia has sold approximately 10,400 DREs to counties within the State of New Jersey. (FOF ¶ 784.) Although the New Jersey market accounts for a somewhat variable percentage of Sequoia's annual sales depending upon sales in other parts of the country, Smith admitted that New

Jersey accounted for roughly 20% of Sequoia's gross annual sales in 2008. (FOF ¶ 784.)

As such, Mr. Smith has admitted that he has a personal stake in the outcome of this litigation, which will affect Sequoia's gross annual sales, and thus will impact Mr. Smith's income, both as an owner of the company and in the amount of his bonus. (FOF ¶ 785.) In fact, this Court has acknowledged Mr. Smith's interest in the outcome of this litigation, and has indicated that Mr. Smith's testimony must be weighted accordingly. (FOF ¶ 786.) Indeed, under the foregoing circumstances, no person logically could be expected to give objective, unbiased testimony.

2. Smith's Trial Testimony Reveals Evidence of Bias

As evidence of Mr. Smith's bias, his trial testimony shows that he could not bring himself to agree with even the most immutable of Professor's Appel's conclusions regarding Sequoia DREs. (FOF ¶ 787.) For example, Mr. Smith disagreed with Professor Appel's assessment that negative vote totals can manipulate elections, an assessment that even Mr. Terwilliger agreed with. (FOF ¶ 787.) In addition, Mr. Smith would not agree with Professor Appel's assessment that problems with the Advantage's daughterboard required immediate attention, which, again, Mr. Terwilliger agreed with. (FOF ¶ 787.) While quick to express disagreement with Professor Appel on this issue, Mr. Smith admitted that he has no expertise, or even familiarity, with flash memory on the daughterboard. (FOF ¶ 787.)

Moreover, Mr. Smith provided chronically inconsistent trial testimony, further revealing his bias. Because of the Defendants' last-minute rebranding of Messrs. Smith and Terwilliger as its experts after the trial had begun, the Court permitted Plaintiffs to re-depose these witnesses. (FOF ¶ 788.) Mr. Smith, however, endeavored to thwart the Court's attempt at a fair solution by holding back testimony at his deposition, and providing inconsistent and sometimes irreconcilable answers to questions posed at both his deposition and at trial. (FOF ¶ 789.) For example, Mr. Smith testified at trial that he is familiar with the 1990 federal voting machine standards. (FOF ¶ 789.) At his deposition, in contrast, Mr. Smith testified: "I'm not entirely familiar with the 1990 standards as they predate me to some degree." (FOF ¶ 789.) Smith attempted to explain this inconsistency by asserting that since his deposition, he had become familiar with the 1990 standards. (FOF ¶ 789.)

Further, Mr. Smith testified at trial that he was able to explain precisely how the Advantage misgenerated party turnout totals during the February 2008 primary election in New Jersey, and that he actually examined that issue personally from the moment it was discovered. (FOF ¶ 789.) At his deposition, however, when asked to explain whether Democratic votes reported in the Republican primary because of the "option switch bug," Mr. Smith answered: "I don't have enough detail familiarity with how the software misgenerated the party turnout totals to answer your question." (FOF ¶ 789.) Mr. Smith also stated during his deposition: "I am not familiar with that level of detail, though I do understand Union County had some issues with their party turnout totals." (FOF ¶ 789.) Mr. Smith did not explain how he went from only a vague understanding that Union County "had some issues" at his deposition, to testifying at trial that he personally dealt with these issues when they were discovered, and to speaking at length about the precise nature and cause of those issues. (FOF ¶ 789.)

By way of further illustration, when asked at trial whether a field programmable gate array chip ("FPGA") could function in the same manner as a Z80 if it is placed into an Advantage DRE, Mr. Smith initially responded: "I do not believe so if it is placed in an Advantage." (FOF ¶ 789.) At his deposition, however, when confronted with the very same question, Smith had answered: "I haven't seen that reduced to practice but in theory, yes." (FOF ¶ 789.) These illustrations serve not as an exhaustive list, but to demonstrate just a few of the many instances in which Mr. Smith's bias and personal interest revealed itself at trial, casting further skepticism on the credence of his testimony. (See FOF ¶ 789.)

3. Defendants' Expert Terwilliger's Personal Interest and Bias

Like Mr. Smith, Mr. Terwilliger has a personal interest in the outcome of this litigation, diminishing the credibility of his testimony. Dating from the time that Mr. Terwilliger worked at Sunrise Laboratories – approximately 18 years ago – all or substantially all of his income has derived from work performed on behalf of Sequoia. (FOF ¶ 790.) From 1997 to 2007, when Mr. Terwilliger was an employee of Sequoia, his bonuses were at least in part a function of the company's sales performance. (FOF ¶ 791.) Mr. Terwilliger currently serves as a consultant for Sequoia, and is working on a firmware modification for the Sequoia Advantage D-10. (FOF ¶ 792.)

Mr. Terwilliger presently has no source of income other than the compensation he receives from Beattie Padovano, Sequoia's counsel in this lawsuit, for his service as an advisor/expert witness in this litigation, and the pay that he receives from Sequoia for his consulting services. (FOF ¶ 793.) Although Mr. Terwilliger was held out as an expert witness for the Defendants, he was not compensated by the Defendants for his services – he was compensated by Sequoia's lawyers! (FOF ¶ 794.) Furthermore, Mr. Terwilliger admitted that although he is purportedly testifying on behalf of the Defendants, he takes his direction from Arthur Chagaris (Sequoia's counsel), Ed Smith, and Michelle Shaffer – Sequoia's Director of Communications. (FOF ¶ 796.)

As if this arrangement were not inappropriate enough based on appearances, Mr. Terwilliger has already demonstrated in a different context that he will perform untoward – and indeed, unlawful – acts at the direction of Sequoia if asked to do so. In 2003, during the course of his employment with Sequoia, Mr. Terwilliger personally registered several Internet domain names consisting of variations on the name "Diebold," which is one of Sequoia's primary competitors. (FOF ¶ 798.)

Mr. Terwilliger admitted that his actions constituted "cyber-squatting."[18] (FOF ¶ 799.) In connection with the registering of these domain names, Diebold filed a legal proceeding against Terwilliger before the World Intellectual Property Organization ("WIPO".) (FOF ¶ 800.) The WIPO panel ruled that the domain names must be turned over to Diebold, finding that Mr. Terwilliger had registered the names in bad faith. (FOF ¶ 801.)

Although Mr. Terwilliger personally registered these domain names, he testified that he did so at the direction of Sequoia officials. (FOF ¶ 802.) Mr. Terwilliger's past willingness to perform unlawful acts at the direction of Sequoia reflects poorly upon the credibility of his testimony in the instant litigation, particularly where he admits that, although an expert for the Defendants, he is taking direction from Sequoia's counsel, Sequoia's Director of Communications, and Mr. Smith.

4. Defendants' Expert Dr. Shamos's Personal Interest and Bias

Defendants' expert Dr. Shamos is also biased. He has a personal financial stake in Sequoia's financial health and thus, in the outcome of this litigation. Dr. Shamos testified that he performs his expert witness work through Expert Engagements, LLC, a company that he and his wife own, and that he is performing his work in this lawsuit through Expert Engagements, LLC. (FOF ¶ 904.) He further testified that 90% of what is paid to Expert Engagements is paid to him, with the remaining 10% going to a joint account shared by Dr. Shamos and his wife. (FOF ¶ 905.) Dr. Shamos is the only expert witness retained by Expert Engagements. (FOF ¶ 906.)

Dr. Shamos has performed, and continues to perform, considerable expert witness work on behalf of Sequoia. He was retained by Sequoia's patent counsel in connection with a prior lawsuit – Avante International Technology v. Sequoia Voting Systems, et al. (FOF ¶ 908) – for which he was

[18] Cyber-squatting is illegal pursuant to the Anti Cyber-Squatting Consumer Protection Act of 1999, codified at 15 U.S.C. § 1125(d.)

paid $525 an hour for a total of between $209,000 and $236,500. (FOF ¶ 910.) Dr. Shamos also was hired by Sequoia's patent counsel to participate in another patent suit by Avante against Sequoia, and expects that he will be hired by Sequoia's counsel for a third patent lawsuit. (FOF ¶ 911.) Dr. Shamos testified that he expects to write expert witness reports for Sequoia in both additional suits, and anticipates that he will most likely spend the same amount of time as he has spent working for Sequoia in the original Avante International Technology v. Sequoia Voting Systems, et al. suit (450 hours) in each of the additional lawsuits. (FOF ¶¶ 912-913.) Dr. Shamos expects to charge Sequoia $525 an hour for his services, and thus expects to be paid at least another $236,250 from Sequoia for each case, for a total of at least $472,500. (FOF ¶ 914.) Clearly then, Dr. Shamos has a personal economic stake in the financial health of Sequoia. This lends skepticism to the objectivity of his testimony in this litigation.

5. Plaintiffs' Experts Are Not Biased

In direct contrast to the personal interests of Defendants' experts in the outcome of this litigation, Plaintiffs' experts have no such interests or biases that could impair the objectivity of their opinions. Professor Appel has worked on this case for nearly five years without compensation. (FOF ¶ 43.) He is working pro bono as a public service, because he views it as part of his role as a computer scientist and a professor in our society. (FOF ¶ 43.) He testified that the role of a professor is not solely to conduct research, teach, and publish, but also is to communicate to the broader public, to society, and to policymakers on research and findings within his expertise and knowledge that are critical to formulating sound public policy. (FOF ¶ 43.) Professor Appel has expressed his willingness to devote whatever time is necessary to communicate to the public and this Court whatever expertise he has bearing on the integrity of elections. (FOF ¶ 44.)

Professor Wolf and Dr. Johnston, like Professor Appel, have received no remuneration from

Plaintiffs for the expert services performed on Plaintiffs' behalf. (FOF ¶¶ 1070, 1217.) Dr. Johnston performed work in this lawsuit because he sees voting integrity as a national security matter. 4/22 Trial Tr. at 157:6-24.

In contrast to Defendants' experts, Plaintiffs' experts' income will not in any way be affected by the outcome of this case. Thus, the opinions of Plaintiffs' experts raise no objectivity concerns, and should be afforded greater weight and credibility by this Court. See Thermographic Diagnostics, Inc.,125 N.J. at 497.

In sum, Plaintiffs' experts are far-better qualified than Defendants' experts to render an opinion in this litigation, as they possess superior credentials, knowledge, and experience, and have no bias or personal interest that could impair the objectivity of their testimony. Moreover, Plaintiffs' experts' opinions are based on solid scientific foundations, including thorough physical inspection of the Sequoia DREs and security seals, and their beliefs are shared by members of the scientific community. The testimony of Plaintiffs' experts should thus be afforded greater credence by this Court than the testimony of Defendants' experts.

VIII. PLAINTIFFS HAVE PROVEN THAT THE USE OF SEQUOIA 9.00H IN ELECTIONS IS UNCONSTITUTIONAL

A. THE RIGHT TO VOTE IS ONE OF THE MOST HIGHLY PROTECTED RIGHTS UNDER THE NEW JERSEY AND FEDERAL CONSTITUTIONS.

Article II, Sec. 1, Para 3 of the New Jersey Constitution states:

> Every citizen of the United States, of the age of 18 years, who shall have been a resident of this State and of the county in which he claims his vote 30 days, next before the election, shall be entitled to vote for all officers that now are or hereafter may be elective by the people, and upon all questions which may be submitted to a vote of the people[.]

The New Jersey Supreme Court has long recognized that the right to vote, guaranteed by the New Jersey Constitution, is one of the most fundamental and important rights in a democratic society. See Gangemi v. Berry, 25 N.J. 1, 12 (1957.) As Chief Justice Weintraub eloquently explained,

> [d]espite an impoverished beginning, the right to vote has taken its place among our great values. Indeed the fact that the voting franchise was hoarded so many years testifies to its exalted position in the real scheme of things. It is the citizen's sword and shield. "Other rights, even the most basic, are illusory if the right to vote is undermined." It is the keystone of a truly democratic society.

Gangemi v. Rosengard, 44 N.J. 166, 170 (1965) (quoting Wesberry v. Sanders, 376 U.S. 1, 17 (1964).)

The United States Constitution also protects the rights of citizens to vote in both state and federal elections. Reynolds v. Sims, 377 U.S. 533, 554-55 (1963.) The right to vote freely is the "essence of a democratic society, and any restrictions on that right strike at the heart of representative government." Id. at 555. The United States Supreme Court has consistently recognized the right to vote as a fundamental one. "Undoubtedly, the right of suffrage is a fundamental matter in a free and democratic society." Reynolds, 377 U.S. at 561-62. "Almost a century ago . . . the Court referred to 'the political franchise of voting' as 'a fundamental political right, because [it is] preservative of all rights.'" Id. at 562 (quoting Yick Wo v. Hopkins, 118 U.S. 356, 370 (1886).)

Because of the fundamental nature of the franchise, it receives special protection. "Especially since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized." Reynolds, 377 U.S. at 562.

B. THE SEQUOIA ADVANTAGE 9.00H VIOLATES THE FUNDAMENTAL RIGHT TO VOTE BECAUSE IT CAN EASILY BE MADE TO SUBVERT VOTER INTENT.

In New Jersey, "[e]lection laws are to be liberally construed so as to effectuate their purpose." Kilmurray v. Gilfert, 10 N.J. 435, 440 (1952.) The right to the franchise includes more protection than simply the right to cast a ballot. "'The right to vote includes the right to have the ballot counted.'" Reynolds, 377 U.S. at 555 n.29 (quoting South v. Peters, 339 U.S. 276, 279 (1950) (Douglas, J. dissenting).) Under the New Jersey and Federal Constitutions, the true intention of the voter must be considered, and respected by election officials and courts.

For example, in In Re General Election Held in the Township of Monroe, the Appellate Division decided to interpret liberally New Jersey voting law to capture the true intention of the voters. 245 N.J. Super. 70 (App. Div. 1990.) In Township of Monroe, voters in a district cast their vote for mayor by both marking his name printed on the ballot and by writing in his name in the write-in portion of the card. Id. at 71. These votes were not counted initially because they allegedly violated N.J.S.A. 19:53A-7(f) (2004) which states: "[i]f the voter has cast more votes for an office than he is entitled to vote for, the vote for that office shall be declared null and void and that vote shall not be counted for that office." Id.

The Appellate Division rejected that rigid interpretation of the statute. The court found that by voting for the same candidate in two places on the ballot the voters did not truly violate this law, and ordered that the votes be counted. Id. at 73. "A contrary ruling would result in disenfranchising voters who clearly demonstrated an intent to vote for one particular person for one particular office." Id.; see also In Re the Petition of Gray-Sadler, 164 N.J. 468 (2000) (setting aside an election where write-in votes were not counted due to poor instructions at the polls, despite the voter's clear intentions); In Re the Petition of Fifteen Registered Voters of the County of Sussex, 129 N.J. Super. 296 (App. Div. 1974) (write-in votes counted where voters used only a first initial or only the last name when identifying their selection.)

As demonstrated by these cases, New Jersey courts have consistently equated the right to vote with the requirement that the true intent of the voters be captured.

Plaintiffs have shown that the Defendants' Sequoia Advantage 9.00H DREs can readily be made to ignore the voter's intent. Professor Appel demonstrated that 9.00H Advantage can be made to mis-record votes, and register votes for the wrong candidate, without detection. His vote stealing program was easy to make, and so thorough that it made sure to cheat in all four internal places where the Advantage stores votes. Additionally, both Professors Appel and Wolf testified that a fraudulent Z80 that cheats in elections is easy to make and almost impossible to detect. Dr. Shamos agrees. When the Sequoia Advantage 9.00H cheats, the voter's true intention is lost and cannot be retrieved. Because New Jersey DREs do not produce a voter-verified paper ballot, and are not otherwise auditable, voter intent can never be ascertained.

Plaintiffs have shown through the testimony of Professor Felten, Mr. Mohoney, Mr. Clayton, Mr. Giles and Ms. Gentile that there is ample opportunity to access DREs to make them cheat. Finally Plaintiffs have shown, through the testimony of Dr. Johnston and Professor Appel that the Defendants' proposed security measures cannot protect against tampering.

Taken together, all this testimony overwhelmingly shows that we have no idea whether the Defendants' DREs count votes as cast, as required by the State Constitution. Such unreliability and insecurity cannot be tolerated given the repeated and consistent holdings of New Jersey Courts that all votes must be counted as voters intended.

IX. PLAINTIFFS HAVE PROVEN THAT BECAUSE RECOUNTS CANNOT BE PERFORMED ON THE SEQUOIA 9.00H THAT THEY VIOLATE BOTH STATUTORY AND CONSTITUTIONAL LAW

A. DREs DO NOT ALLOW A "RECOUNT OF VOTES CAST AT THE ELECTION" AS REQUIRED BY NEW JERSEY STATUTES.

Title 19 lays out detailed instructions for the recount of paper ballots (which, of course, would include voter-verified paper ballots), ballot cards and lever-cast votes. In contrast, no instructions are given on how to perform recounts of votes cast using DREs.

N.J.S.A. 19:28-1 provides that a candidate who believes an error has been made has the rights to apply to a judge of the Superior Court for a recount. If the judge determines that a recount is necessary, the judge orders a public recount by the county elections board in the judge's presence. N.J.S.A. 19:28-3.

The judge determines the terms under which the recount is conducted, and decides any disputed questions that cannot be resolved by a majority vote of the county board of elections. Id. The elections board attends the recounting under subpoena, "witness[es] the opening of the ballot box or boxes," and may subpoena witnesses and evidence. Id. Each ballot box used in the recount contains all ballots cast, spoiled, unused or rejected at the election, as well as one tally sheet, as provided in N.J.S.A. 19:18-1 (Election records placed in ballot box.)

Similarly, votes cast using an optical-scan system (used for provisional and absentee ballots in all counties) are recounted by repeating the optical scanning process described in N.J.S.A. 19:53 A-8. This includes producing duplicates for defective ballot cards (as necessary), and counting some or all votes manually if the county board of elections determines it is impracticable to complete the count mechanically. Additionally, a court may order a manual recount of ballot cards. N.J.S.A. § 19:53A-14.

Moreover, 19:48b(1) requires that in the case of recounts, when DREs with voter-verified paper ballots are used, the paper ballot counts as the official ballot. Without further guidance, the presumption is that the paper ballot would be counted in the same way as the other paper ballots listed above.

Although lever machines can no longer be used in New Jersey, protocols existed to conduct recounts using those machines. N.J.S.A. 19:52-6:

> The judge shall . . . order the machine in question opened and the registering counters rechecked against the election officers' returns . . . under the supervision of the county election officials and in co-operation with the parties at interest or their representatives.

The particular "manner of rechecking machines" is spelled out in more detail in N.J.S.A. 19:52-6.1. That statute describes the unpacking and unlocking of the machine, the opening and reading of the counters, the compilation of tally sheets and their comparison to the original election records. See generally N.J.S.A. 19:52-6.1; see also Theurer v. Borrone, 81 N.J. Super. 188, 191 (L. Div. 1963) *aff'd* 85 N.J. Super. 142 (App. Div. 1964.)

Counting votes cast on paper or ballot card, or by physically moving a lever, is a simple process of examining a physical artifact of voter intent. Thus, counting and recounting can be observed easily by the public.

Lever-machine counters, although they produce no paper verification, still produced very reliable recount information. Counters in lever machines are advanced through a simple, verifiable mechanical process. The physical effects of that process, consisting of the observable movement of the counters, can be easily observed. The relative internal simplicity of a lever machine allowed the Appellate Division to determine that the results of a local election were misreported due to a specific and easily-proven mechanical malfunction. See Application of Moffat, 142 N.J. Super. 217, 222 (App. Div. 1976) (Shaft connected to counter wheel registering votes for a candidate "became dislodged, so that the wheel failed to move after the first vote was cast for him.")

In sharp contrast to lever machines, optical scanners and human counters, recounts on paperless DREs cannot be verified in anyway. As Professor Appel demonstrated, a DRE could take votes cast for candidate "A" and record them as votes for candidate "B" without leaving a trace. (See FOF ¶ 39; 66-100.) Its subsequent confirmation of its own inaccurate record would be a mere reprint masquerading as a recount. At best, DREs asked to perform a recount will state the same result they stated once before. This is very different from demonstrating that their original statement was accurate. Accepting a reiteration of previous conclusions about electoral results in lieu of a recount is incompatible with New Jersey statutory law.

Additionally, reliance on a vendor's assistance in the event of a recount would be anathema to New Jersey law. A vendor's assurances that it should be trusted to accurately process and honestly report electoral data begs the question every recount is designed to answer: whether the votes were recorded accurately in the first place. New Jersey statutes, including the voter-verified paper ballot law clearly and consistently require visible and tangible proof of voter intent.

By producing no evidence of voter intent that can be independently verified, paperless DREs function in direct opposition to the spirit and letter of New Jersey law concerning recounts.

B. IN THE EVENT Of A RECOUNT, DRE VOTERS HAVE NO ASSURANCE THAT THEIR VOTES WILL BE TREATED THE SAME AS VOTES CAST VIA ABSENTEE AND EMERGENCY PAPER BALLOTS. THIS UNEQUAL CONSIDERATION OF VOTES VIOLATES THE RIGHT TO EQUAL PROTECTION GUARANTEED BY THE NEW JERSEY CONSTITUTION.

The mere fact that specific guidelines exist in Title 19 for recounting votes cast on paper ballots, ballot cards and lever machines, but not for votes cast on DREs, denies DRE voters the right to equal protection guaranteed by the New Jersey Constitution.

Votes cast on DREs do not produce tangible evidence of voter intent, and therefore cannot be "recounted" like paper ballots, ballot cards or the observable movements of a lever-based voting machine. This means that, in the event of a recount, the votes of those who do not vote on DREs, who make up a minority of voters, will determine the outcome of the election, as those are the only votes that can be verified independently.

Should any recount be needed, voters using DREs will have no option but to rely on printed summaries of encoded data from machines that are prone to manipulation and error. DRE voters have no firm assurance that their votes will be actually recorded and recounted. Indeed, there are no guidelines whatsoever to guide county officials in performing a recount where DREs have been used.

In sharp contrast, all New Jersey citizens who vote by absentee, emergency, or provisional ballot are guaranteed to have their votes counted in the event of a recount, even if they reside in counties that are using DREs. Joanne Rajoppi testified that in the event of a recount, it is the emergency ballots and absentee ballots that are recounted until a winner is declared, (2/26 Trial Tr. at 93:6-11), and Robert Giles testified that there is no statewide policy for conducting recounts, (FOF ¶ 723.)

This unequal treatment of voters in the event of a recount violates the right to equal protection guaranteed by the New Jersey Constitution. Article 1, Paragraph 1 of the New Jersey Constitution protects against "the unequal treatment of those who should be treated alike." Greenberg v. Kimmelman, 99 N.J. 552, 568 (1985.) In comparison to the equivalent Fourteenth Amendment guarantees, "our State Constitutions have been construed to provide analogous or superior protections to our citizens." Peper v. Princeton Univ. Board of Trustees, 77 N.J. 55, 79 (1978.)

In analyzing equal protection challenges, New Jersey courts have rejected the rigid approach followed by the federal courts. Instead, New Jersey courts rely on a flexible three-part balancing test to determine whether an action violates equal protection. Barone v. Dep't of Human Services, 107 N.J. 355, 368 (1987) (quoting Borough of Collingswood v. Ringgold, 66 N.J. 350, 370 (1975), appeal dismissed, 426 U.S. 901 (1976).) The test examines "the nature of the affected right, the extent to which the governmental restriction intrudes upon it, and the public need for the restriction." Greenberg, 99 N.J. at 567. New Jersey's equal protection analysis requires "a real and substantial relationship between the classification and the governmental purpose which it purportedly serves." Taxpayers Ass'n of Weymouth Township v. Weymouth Township, 80 N.J. 6, 55 (1976.)

In the event of a recount, the equal protection rights of DRE voters will be violated. Here, the nature of the voters' affected right, to have their votes counted, is of the highest magnitude. The right to vote is constitutional and fundamental. "A citizen's constitutional right to vote for the candidate of his or her choice necessarily includes the corollary right to have that vote counted 'at full value without dilution or discount.'" Gray-Sadler, 164 N.J. at 474 (quoting Reynolds, 377 U.S. at 555 n.29 (quoting South v. Peters, 339 U.S. at 279 (Douglas, J., dissenting)).)

The second Greenberg factor is the extent to which use of DREs intrudes upon the affected right. In the case of a recount, the intrusion is total. As discussed at length above, the right to have election officials publicly examine the votes cast cannot be honored where there is no observable physical product of the voting process, but merely a reiteration of a biased technician's conclusion. Non-DRE voters enjoy the security of knowing their votes will be examined and confirmed in a recount. DRE voters do not.

The final Greenberg factor examines whether the restriction addresses any public need. The focus is "whether there is an appropriate governmental interest suitably furthered by the differential treatment" embodied in the complained-of action. Barone, 107 N.J. at 368 (quoting Ringgold, 66 N.J. at 370.) There is no public benefit in recording votes on a DRE that can readily be made to cheat in perpetuity without being caught.

Voting systems that do not generate a physical piece of paper that indicates voter intent cannot recount votes in a manner consistent with the spirit and letter of New Jersey election law. In the event of a recount, fraud or error in the computation of DRE vote totals cannot be detected, and the true intent of the voters cannot be confirmed. The inability to confirm the intent of DRE voters in a recount exposes those voters to a significant risk of disenfranchisement not shared by other voters. This inequality concerning the protection of a fundamental right violates the equal-protection rights of DRE voters under the New Jersey Constitution.[19]

X. THIS COURT SHOULD DE-COMMISSION THE DEFENDANTS' DREs IMMEDIATELY AND ORDER THE DEFENDANTS TO USE PRECINCT-BASED OPTICAL SCANNERS THAT COUNT HAND-MARK PAPER BALLOTS

A. THE ONLY WAY TO TRUST ELECTION RESULTS IS IF VOTING MACHINES ARE SOFTWARE INDEPENDENT

The New Jersey public, acting through the legislature, supports verifiable elections. In 2005, it passed a law requiring voter-verified paper ballots. N.J.S.A. § 19:48-1(b) (1.)[20] Even when there is no suspicion of tampering, testing a small but statistically significant sample of all precincts by recounting them could ensure a high probability that the overall result was honest and that widespread fraud or error would be detected. (FOF ¶ 416.) Indeed, the New Jersey legislature passed a law requiring exactly this kind of random audit. N.J.S.A. § 19:61-9 (requiring creation of independent audit team to use statistical science methods to ensure accuracy of elections.) The provisions of N.J.S.A. § 19:61-9 require hand-to-eye verification of paper ballots, which clearly presupposes the existence of such ballots. N.J.S.A. § 19:61-9(a.)

The existence of voter-verified paper ballots is not just the law. It is also a good idea. Because the modalities of fraud or error vary greatly between the counting of paper ballots and the behavior of computer software, each form of counting acts as a check on the other. (FOF ¶ 418.) An attacker would face great difficulty attempting to steal elections in systems with voter-verified paper records. (FOF ¶ 418.)

[19] Plaintiffs do not assert a federal constitutional claim, but note that Bush v. Gore, 531 U.S. 98, 109 (2000) established that inconsistencies in recounting can violate citizens' Equal Protection rights as guaranteed by the Fourteenth Amendment of the United States Constitution.

1. Software Independence is Critical in any Computer-Based Voting System

The Sequoia AVC Advantage 9.00H lacks any voter-verified paper ballot or independent audit trail or other way to verify that its contents are accurate. (FOF ¶ 52.) The only record of the election is the vote totals the DRE itself provides at the end of the day. (Id.) Therefore, it is a "black box" with no verifiable accuracy. As such, like all other computers, the Sequoia AVC Advantage 9.00H DRE can be programmed to do whatever the programmer tells it to do, and is inherently insecure and unreliable. (FOF ¶ 52.) Software independence is considered the superior means of ensuring the electoral accuracy of any computer based system. (FOF ¶ 403.)

Software independence in electronic voting requires being able to verify vote totals computed by a voting machine independently of the computer program used to count them. (FOF ¶ 420, 402.) Among experts in the field of computer security who study voting systems, the only currently commercially available technology which achieves software independence is the voter-verified paper ballot. (FOF ¶ 404.)

A voter-verified paper ballot is an individual paper record of every vote cast, seen and verified by the voter at the time the vote is cast, and saved in a ballot box or bag so that the paper ballots can be recounted by hand if suspicions arise as to the totals. (FOF ¶ 415.) Even, Mr. Smith testified that "software independence" is vital to secure voting machines in New Jersey. (FOF ¶ 840.) The consensus of the computer security community is that without software independence a voting system cannot be trusted. (FOF ¶ 405.)

Dr. Shamos, a staunch supporter of paperless voting systems (FOF ¶ 926) admitted several times during the trial that he is alone in the scientific community in his support of that system. (FOF

[20] The State legislature subsequently, in 2009, conditionally suspended these provisions until funds are available. N.J.S.A. § 19:48-1(b) (2.)

¶ 927-929; 1051; Shamos Test., 3/25, Trial Tr., 135:2-6; 136:2-21; 137:11-16.)[21]

Systems with software independence are the only way to provide the New Jersey electorate with confidence that the Defendants' 11,000 DREs are not infected with viruses. (Appel Test., 4/14 Trial Tr. at 48:6-11.)

2. Precinct-based Optical Scanners are the Best Form of Software Independent Voting Systems

There are three commercially available forms of voter-verified paper ballot: hand counted paper ballots, optical-scan ballots counted by computer, and paper ballots printed by a printer attached to a DRE. (FOF ¶ 419.) It is the overwhelming consensus of computer scientists who have studied voting technology that the most trustworthy, robust, and reliable form of voter-verified paper ballot is the precinct-count optical-scan ballot. (FOF ¶ 420.) Indeed, optically scanned ballots are the only true form of software impendence. Mr. Terwilliger admitted that unlike optical scan voting, where the voter marks the ballot directly, Sequoia's audit trail for their AVC Advantage is dependent on software. (FOF ¶ 841.)

While optical-scanning systems are computers, like DREs, that can similarly be hacked, there is a paper record of the election with precinct-count optical-scanning systems which can be compared against the computer tally. (FOF ¶ 425.) Each method of tallying can be used to check the accuracy of the other. (FOF ¶ 425.) By contrast when a paperless DRE is hacked, there is no recourse. (FOF ¶ 425) There is no way to audit the results (FOF ¶ 425) as required by New Jersey statutory law.

There are two typical ways to count optical scan ballots. The less favored method is to gather

[21] In his rebuttal testimony, Professor Appel testified that he actually spoke to the individuals who Dr. Shamos stated supported parallel testing and that all of them stated that parallel testing was inferior to software independence, DREs with voter-verified paper audit trails, and precinct based optical scanners. (FOF ¶ 1033.) Professor Appel read

the ballots from many precincts to a central location at the end of the voting day and then count the ballots in bulk with a high speed scanning computer. (FOF ¶ 421-422.)

The preferred method is the precinct-count method, in which a person, usually the voter herself, places the completed ballot into an optical scanning machine located in the polling place. (FOF ¶ 423.) The precinct-count method is favored for a number of reasons related to security and accuracy. These include:

- If the voter feeds an overvoted or otherwise invalid ballot into a precinct-count optical scan, the machine spits it back out with an informational message explaining the error. The voter is offered an opportunity to correct it immediately, practically eliminating accidental overvoting.[22] (FOF ¶ 424.)
- Precinct-count optical-scanners deliver a total immediately upon the close of the polling place, while witnesses are still present, ensuring security, reliability, and a clean chain of custody. (FOF ¶ 425.)
- By comparison, central-count optical scanning systems require election workers to transport ballot boxes to a central location, introducing opportunities for unobserved manipulation, ballot box stuffing, and substitution of altered ballots. (FOF ¶ 425.)

Optical scan voting also has quite substantial advantages over DREs with paper-ballot printers, including, but not limited to, the following:

- Using a paper ballot, voters actually personally examine and create the ballot which they present to the machine. While there is uncertainty about how closely people examine paper ballots printed by a DRE, there is no question that voters have examined an optical-scan ballot since they made the marks themselves. (FOF ¶426.)
- All voting machines can malfunction. When a DRE stops working, voters are completely unable to vote. However, if a precinct-count optical-scan machine breaks, voters can continue filling out paper ballots at the same rate of speed, saving them in a ballot box for later counting, after the machine is repaired or replaced. (FOF ¶ 426.)

the Brennan Center for Justice report's conclusion to the Court that parallel testing was inadequate and inferior method or protecting the integrity and accuracy of elections and voting machines. (FOF ¶ 1033.) See Exh. P-75.

[22] There is usually an override which allows a voter to cast the ballot anyway. (Appel Report, § 67.12 n. 128, at 142.)

- Only one voter at a time can use a DRE. When ballots are complicated or contain many candidates or ballot questions, this can greatly slow down the voting process. By comparison, multiple voters can fill out their paper ballots at the same time, given any booth containing nothing more than a flat surface and a pencil, costing virtually nothing. Then, when the voters have finished filling out their ballots, they emerge and feed their ballots into the optical-scanner. (FOF ¶ 426.)
- DREs with attached printers create a difficult situation for poll workers when a voter claims the printout doesn't match their vote. Either the DRE is malfunctioning or the voter is mistaken, or even lying. However, the poll worker has no way to figure out which, since watching the voter cast her votes would invade the privacy of the voter. By comparison, there is no doubt about where the marks are on a paper ballot. The voter made those marks with a pencil herself. (FOF ¶ 426.)
- DREs, as Professor Appel has demonstrated repeatedly during the course of this trial, often have confusing and ambiguous user interfaces. By comparison, the use of paper and pencil are intuitively obvious to voters, and when the optical-scanner accurately reports their vote to them, they can be confident that their vote has been counted. (FOF ¶ 426.)

Precinct-count optical scan systems are more cost-effective than paperless DREs, because precincts need fewer optical scanning voting machines than DREs. (FOF ¶ 432.) Further, fewer DREs are required because the cost of machine failure for optical scanning machines is much lower. (FOF ¶ 432.) DRE failure can lead to a total shutdown of the polling place, or long lines, driving away voters who are unwilling to wait for the two hours or more it takes to send out a spare. (FOF ¶ 432.) While it is still a good idea to have two optical scanners at each precinct in case of failure, even a failure of both scanners would not shut down the polling place. (See FOF ¶ 432.)

Professor Appel studied the error rate of the precinct-based optical scanners by studying all the data related to the total hand count of optically scanned paper ballots used in the 2008 Minnesota Senate race. (FOF ¶ 427.) Professor Appel testified that the error rates of the precinct-based optical scanners was one hundredth of one percent or one in 10,000 ballots. (FOF ¶ 430.) This means that the accuracy of the precinct-based optical scanners was 99.99%. (Professor Andrew Appel, *Optical-*

scan voting extremely accurate in Minnesota, Jan. 28, 2008, http://www.freedom-to-tinker.com/blog/appel/optical-scan-voting-extremely-accurate-minnesota) (last visited, June 26, 2009.)

The overwhelming majority of computer scientists and other election technology experts have concluded that precinct-count optical-scan systems are the most trustworthy, robust, and cost-effective method of voting that is now available. (FOF ¶ 405.) Professor Appel recommends that New Jersey adopt precinct-count optical scan technology. (FOF ¶ 420.)

B. ORDERING A SPECIFIC REMEDY THAT PRESERVES THE FUNDAMENTAL RIGHT TO VOTE, WHEN THE STATE HAS ADMITTED THAT IT WILL NOT PROTECT THAT RIGHT, IS WITHIN THIS COURT'S POWERS.

1. The State Is Seeking To Squander $19 Million Dollars That Could Be Used To Purchase Auditable DREs.

Robert Giles testified that since 2002, New Jersey received between $80-$90 million in federal funds under the Help American Vote Act (HAVA, Pub. L. 107-252, 115 Stat. 1274, 1279, 116 Stat. 1666, et. seq.) to upgrade its voting systems and election administration. (FOF ¶ 737.) Approximately $19 million of these funds remain. (FOF ¶ 738.) New Jersey is eligible to receive an additional $6.2 million in required HAVA payments for 2008-09. (NJ Div. of Elec., Preliminary HAVA Plan Second Addendum 1, *available at* http://www.njelections.org/havanj/nj -preliminary-hava -addendum.pdf) (last visited, June 20, 2009) (hereinafter "HAVA Plan Addendum".)

Mr. Giles testified that the HAVA funds could be used "to replace New Jersey's voting machines with a different kind of system that is more accurate and reliable." (FOF ¶ 739.) HAVA expressly considered such purchases (HAVA, Sec. 101(b) (1) (F), 42 U.S.C. 15301), and N.J.S.A. 19:48-1 and 19:53A-3(i) (2008) require that all voting machines produce voter-verified paper ballots.

HAVA requires that states submit a "State Plan" which demonstrates HAVA compliance and the contemplated use for the funds. (HAVA, Sec. 251-256, 42 U.S.C. 15401-15406; see also N.J. Div. of Elec., "State Plan: Improving the Shape of New Jersey's Voting Experience" 1, Sep. 15, 2003, available at http://www.njelections.org/havanj/hava_state_plan_9.19.03.pdf) (hereinafter "HAVA Plan Addendum") (last visited June 20, 2009.)

In 2007, the State earmarked $15 million in HAVA funds to implement the voter-verified paper audit trail on voting machines. (HAVA Plan Addendum, at 1:3.) These plans were never effectuated. Indeed, on March 6, 2009, upon the Defendants' request, the Legislature suspended the implementation of the voter-verified paper ballot requirements of N.J.S.A. 19:48-1 and 19:53A-3(i) until funds were made available to purchase voting technology which ensures each voting machine produces an individual permanent record of every vote cast. (N.J.S.A. 19:48-1(b) (2), Pub. L.2009, c.17, §1 (March 6, 2009); N.J.S.A. 19:53A-3(i) (2), Pub. L.1973, c.82 (March 6, 2009).)

Even though the $19 million in HAVA funds could be used to purchase New Jersey's voting machines that are software independent and compliant with the law (FOF ¶ 738.), the Defendants now seek to reallocate $15 million of the HAVA funds for other purposes.

On June 3, 2009, the Defendants published alterations to their plan for the $19 million remaining in HAVA funds. (HAVA Plan Addendum.) The new State Plan allocates $2 million towards purchasing DRE voting machines for counties with new election districts due to population increases, and $13 million for what the Defendants call "HAVA required mandates." (HAVA Plan Addendum, at 1.) The Defendants plan to spend a $8 million for general improvements to the Statewide Voter Registration System (SVRS) (HAVA Plan Addendum, at 2); $4 million for the development of an online help desk to serve counties and voters (HAVA Plan Addendum, at 2);

more than $3 million in "State management costs" including salaries (HAVA Plan Addendum, at 2-3); and $1 million each for website enhancements, online poll worker training, voter education and outreach, and technological improvements to SVRS to assist counties with decennial redistricting. (HAVA Plan Addendum, at 2-3.)[23] The public comment period for the State's plan ends on July 3, 2009. (HAVA Plan Addendum, at 2.)

The $19 million of remaining HAVA money can and should be used towards the purchase of voting machines that will satisfy the public's and legislature's will for voter-verified paper ballots and redress the statutory and constitutional deficiencies of the Sequoia Advantage 9.00H. If the Defendants were to reallocate the funds according to June 3rd plan, it would be diverting money that is sorely needed to replace DREs that violate state law and use it for items that do not need immediate remediation (because they are not constitutional violations.) Diverting part of the $19 million to purchase even more DREs that are unconstitutional and to train poll worker and voters on how to use them is a waste of money.

Additionally, buying more unconstitutional DREs is wasteful because DREs may soon be obsolete. On June 16, 2009, Representative Rush D. Holt (D-NJ) introduced federal legislation to end the reliance on DREs nationwide and require voter-marked paper ballots. (Voter Confidence and Increased Accessibility Act of 2009, H.R. 2894, 111th Cong., §§301 (a) (2) (2009.) At the writing of this document, the bill has 80 co-sponsors, including seven Congressmen from New Jersey, (five Democrats and two Republicans.) H.R. 2894 has been referred to the House Committee on Science and Technology.

Should the momentum behind Representative Holt's bill continue to build, all of the

[23] The HAVA Plan Addendum includes a spreadsheet which slightly alters the presentation of the State's plan. Specifically, the spreadsheet combines two allocations each for SVRS ($9 million increase), voter education and outreach ($2 million increase), and the training of election officials ($5 million increase.) (HAVA Plan Addendum, at 3.)

Defendants' DREs would become obsolete. Thus, using HAVA funds the purchase of new Advantage 9.00H is truly squandering precious HAVA funds still available to New Jersey.

2. When Major Constitutional Issue Are At Stake, The Court May Compel Specific Appropriations.

The Defendants, through their five year failure to put into place auditable voting systems, has made it clear that it refuses to comply with the Legislature's voter-verified paper ballot mandate, or to fund that mandate. Thus, it is critical for this Court to order that funds be set aside to purchase voting systems that comply with the State's voting rights laws.

The New Jersey Supreme Court has held repeatedly that where a constitutional right is in danger of being violated, the judiciary has the authority and duty to direct the legislature how to appropriate State funds. Robinson v. Cahill is the seminal case in that regard. 67 N.J. 333 (1975.) Robinson provides authority for this Court to direct the Legislature to appropriate monies to rectify New Jersey's insecure and inaccurate DREs to produce a voting verified paper ballot. In Robinson, the New Jersey Supreme Court held that the courts are obligated to act when the other branches of government fail to protect a constitutionally guaranteed right. Id. at 347. In fact, the opening sentence of the Robinson decision states emphatically that "[t]he Court has now come face to face with a constitutional exigency involving, on a level of plain, stark and unmistakable reality, the constitutional obligation of the Court to act." Id. at 339.

In Robinson, plaintiff parents showed that the Defendants failed to ensure the constitutional mandate that all children receive equal educational opportunities. See id. at 343-44. They argued that the Defendants failed to provide for the maintenance and support of a constitutionally-mandated "thorough and efficient" system of free public school education for all children. Id. As a remedy, the Court ordered the legislature to disburse educational funds according to a particular formula taken from previous legislation to ensure that all students received equal educational opportunities.

Id. at 341, 354.

The Court rejected the Defendants' argument that judicial intervention in appropriations from the State Treasury violated the separation of powers doctrine. Id. at 344. The Court provided several reasons for doing so. First, the Court noted that the legislature cannot curtail the constitutional rights of citizens by its inaction. Id. at 347. Second, the Court found that the New Jersey judiciary has traditionally taken affirmative action to protect constitutional rights. Id. at 352 (citing to Jackman v. Bodine, 43 N.J. 453 (1964) ("Jackman I"); Swann v. Charlotte-Mecklenburg Bd. of Educ., 402 U.S. 1 (1971); Griffin v. School Bd. of Prince Edward County, 377 U.S. 218, 233-34 (1964); Hawkins v. Shaw, Mississippi, 437 F. 2d 1286 (5th Cir. 1971); Kennedy Park Homes Ass'n v. Lackawanna, N.Y., 436 F. 2d 108 (2d Cir. 1970), *cert. den.* 401 U.S. 1010 (1971); Mills v. Bd. of Educ., 348 F. Supp. 866 (D.D.C. 1972).) The Court noted that:

> When there occurs such a legislative transgression of a 'right guaranteed to a citizen, final decision as to the invalidity of such action must rest exclusively with the courts. It cannot be forgotten that ours is a government of laws and not of men, and that the judicial department has imposed upon it the solemn duty to interpret the laws in the last resort. However delicate the duty may be, we are not at liberty to surrender, or ignore, or to waive it.'

Id. at 347 (quoting Asbury Park Press, Inc. v. Woolley, 33 N.J. 1, 12 (1960).) The Court further noted that the judiciary's responsibility to safeguard the rights of individuals is "as old as this country." Id. at 347. Finally, the Court found that:

> This Court, as the designated last-resort guarantor of the Constitution's command, possesses and must use power equal to its responsibility. Sometimes, unavoidably incident thereto and in response to a constitutional mandate, the Court must act, even in a sense that seems to encroach, in areas otherwise reserved to other branches of government.

Id. at 354 (quoting Powell v. McCormick, 395 U.S. 486 (1969).)

The New Jersey Supreme Court determined that immediate judicial intervention was necessary, even though there were indications that the Legislature and the Executive branches had already begun to correct for the constitutional deficiency. Id. at 344. That the Legislature had begun to take steps only affected the duration of the Court's provisional remedy. Id. at 344, n. 4.

The Court also found that where there is a "theoretical conflict" between the Constitution's Education Clause and the Constitution's clause giving the legislature appropriations power, that it was the Court's duty to enforce the Education Clause. Id. at 354.

New Jersey courts have fashioned very specific remedies for the legislature in a number of instances, including where the right to vote was being compromised. In Jackman, the Court determined that the New Jersey Legislature was not apportioned in a way that protected the right to "one person, one vote," as guaranteed by the Constitution. Id. at 459. The Court took the bold but necessary step of enjoining all elections until the Defendants' apportionment system was changed. Id. at 478. The Jackman I Court directed the Legislature to devise a new apportionment system through a constitutional convention. The Court reserved the right to intervene if the Legislature did not make the appropriate changes within a limited time frame. This very specific remedy was affirmed in Jackman v. Bodine, 44 N.J. 312 (1965) ("Jackman II".)

The New Jersey Supreme Court's holdings in Robinson and both Jackman opinions clearly apply to this case. First, as in both Robinson and Jackman I, the right at stake here (the right to vote) is fundamental and protected by the New Jersey Constitution. See N.J. Const. (1947), Art. II, §1, para. 3. Because it is impossible to know whether New Jersey's DREs are counting votes correctly, they violate the right to vote and to have one's vote counted accurately which are guaranteed by the New Jersey Constitution and Title 19. See e.g., New Jersey Democratic Party v. Samson, 175 N.J. 178, 187 (2002) (citing Reynolds v. Sims, 377 U.S. 533, 555 (1964) (implicit to right to vote is right to have vote counted as cast).)

Second, as in Robinson and Jackman I, the constitutional right is being violated on a statewide basis. Essentially almost all of New Jersey DREs are unreliable, not thoroughly tested and insecure. They do not (and cannot) produce a voter-verified paper ballot – which makes them unauditable. The overwhelming evidence presented at trial shows that there is no way to know whether the 11,000 Sequoia Advantage DREs are counting or manipulating votes. Such uncertainty and utter lack of transparency in voting severely compromises the right to vote. The Court in Robinson stated that where a fundamental right guaranteed by the Constitution is at stake, the Court must "afford an appropriate remedy to redress a violation of those rights. To find otherwise would be to say that our Constitution embodies rights in a vacuum, existing only on paper." Robinson, 67 N.J. at 347 (citations omitted.)

Third, the Court in Robinson and Jackman I took action after the Legislative and Executive Branches failed to take decisive steps to correct for the constitutional defects in its educational system. In Robinson, the Court's remedy was in the form of provisional relief. The Court required that educational funding for the 1976-1977 academic year be revised according to a new formula. If the Legislature resolved the issue of unequal education before the end of that year, then a judicial remedy would no longer be required.

The Court devised a similar remedy in Jackman I. The Court established time limits for the Legislature to correct for its inadequate representation and structure through a constitutional convention. Jackman I, 43 N.J. at 476-77. The Court found that if the issue of unequal legislative apportionment remained unresolved after the convention, it would intervene by adopting and enforcing a plan of its own design. Jackman II, 44 N.J. at 316-17. The Court determined even "the call of a constitutional convention is not a fact which would relieve us from our obligation to abide by the mandate of the highest court in the land." Id. at 316.

Like in Robinson and Jackman I, this Court has the authority to fashion a remedy to protect the constitutionally guaranteed right to vote. Immediate action is needed because the Defendants seeks to squander $19 million dollars in HAVA funds that could be used to purchase auditable DREs to buy more 9.00H DREs and to train poll workers to use those DREs which are unconstitutional and obsolete under State law.

This Court also has the authority to mandate that funds be set aside to bring New Jersey voting machines into compliance with the Constitution and Title 19. This is particularly true because § 19:53A-3.1 makes clear that the Defendants must pay for bringing voting machines into compliance with the voter-verified paper ballot requirement.

3. This Court Has The Authority To Take Specific Action To Protect The Franchise.

The protection of voting rights squarely within the authority of the judiciary. Title 19 specifically authorizes the judiciary to ensure that approved voting systems are reliable and comply with fifteen specific security requirements in N.J.S.A. § 19:48-1 (a)-(o.) Furthermore, N.J.S.A. § 19:48-2 charges the judiciary with reviewing the certification of voting machines.

As the Defendants' Chief Election Officer, the Secretary of State is charged with protecting the right to vote by ensuring that all voting machines are equipped to produce a voter-verified paper ballot. When the Chief Election Officer fails to honor that obligation, as it has been the case for five years, the judiciary may – and indeed is obligated – to intercede.

In fact, New Jersey courts have intervened in elections, which are ordinarily under the auspices of the executive branch, to protect the integrity of the electoral process. For example, courts have consistently set aside elections where there is evidence of tainted results caused by malfunctioning voting machines. When machines fail to work properly, judicial action is necessary to protect New Jersey voters' constitutionally-protected rights. See, e.g., In Re Petition of Hartnett, 163 N.J. Super. 257, 268 (App. Div. 1978); In Re the Application of Moffat, 142 N.J. Super. 217, 222 (App. Div. 1976) (court intervention ensued when a voting machine malfunction caused a recording mechanism within the voting machine to become dislodged); In Re the 1984 General Election for the Office of Council of the Township of Maple Shade, 203 N.J. Super 563 (Law Div. 1985) (setting aside election even though alternative voting methods, such as emergency ballots, were available to voters, because those voting measures were not properly implemented.)

Additionally, as discussed above, in Jackman I, the New Jersey Supreme Court found that when the legislative branch does not protect voters' constitutionally guaranteed right to vote, the judiciary is obligated to intercede. The Jackman I Court refused to honor the legislature's request that it refrain from adjudicating the case. 43 N.J. at 457-58. Thus, clearly, it is within the Court's powers to order the legislature to revamp its structure, hold a constitutional convention, and enjoin elections until legislative apportionment complied with the Constitution. See id. at 476-78; see also Robinson, 67 N.J. at 344.

Hartnett, Moffat, and Jackman demonstrate the great lengths the New Jersey judiciary has taken to ensure that every vote is counted. Given its broad mandate to uphold the Constitution and laws of New Jersey, this Court is empowered to avert serious harm to New Jersey voters. Indeed, it is within both this Court's legal and expansive equitable powers to provide relief to in furtherance of the public interest. Texas Co. v. Di Gaetamo, 71 N.J. Super. 413, 430 (App. Div. 1962) (quoting Mercoid Corp. v. Mid-Continent Inv. Co., 320 U.S. 661, 670 (1944) (internal quotations omitted).) Clearly, there is no greater public interest than preserving our fundamental right to vote, which is being violated by the 11,000 Sequoia AVC 9.00H Advantage DREs used throughout the State.

4. The Sequoia Advantage D10 Is Not An Adequate Remedy

Replacing Sequoia Advantage DREs currently in use with the Sequoia Advantage D10 is an insufficient remedy to redress the statutory and constitutional infirmities of the Advantage 9.00H.

The Sequoia Advantage D10 is even more insecure than the Advantage 9.00H because the Advantage D10 stores all of its firmware in rewritable flash memory on the daughterboard. (FOF ¶ 69.) Defendants' witnesses concede that the flash memory on the D10 daughterboard is unsafe. Paul Terwilliger of Sequoia admits that the data on the daughterboard's flash memory is vulnerable to being changed or overwritten. (FOF ¶ 271.) Dr. Shamos, Defendants' expert witness, wrote in his Rebuttal Report that the severe vulnerability of the daughterboard is completely unacceptable and requires "immediate remediation." (FOF ¶ 272.)

Infecting the Sequoia Advantage D10 with fraudulent firmware does not require physical access or contact with the DRE (FOF ¶ 274.) Indeed, simply inserting a PCMCIA cartridge containing fraudulent firmware into an easily accessible slot on the outside of the DRE causes the daughterboard to automatically overwrite the legitimate daughterboard firmware with the fraudulent firmware from the cartridge. (FOF ¶¶ 233, 235, 269.) A single infected PCMCIA card can infect every WinEDS computer and every Advantage D10 used in the State.

A fraudulent vote stealing card can be inserted on purpose, or inadvertently by a well-meaning election worker. Such a program could be written on the credit-card sized daughterboard "results cartridge" that is used to store election results and upgrade the D10 DRE's firmware. (FOF ¶275.)

Consequently, the firmware on the Advantage D10 daughterboard can be manipulated to change the votes of all voters. Fraudulent firmware on the daughterboard would change the votes before they were transmitted to the motherboard and the fraud would be undetectable.

The enhanced vulnerabilities inherent in the flash memory of the D10 makes that version of the AVC Advantage even more legally infirm than the version 9.00H examined by Professor Appel. As such, the Court should not consider it as a remedy in this case. The Defendants' 9.00H DREs should be replaced with software independent auditable systems that are secure. As discussed above, the best software independent system is the precinct-based optical scanner.

CONCLUSION

Plaintiffs have demonstrated that New Jersey's 11,000 Sequoia Advantage DREs, WinEDS tabulation system, results cartridges, and county networks carrying election results and ballot information are all vulnerable to attack. Hackers who have physical access to the DREs and attackers who spread viruses remotely can alter votes in New Jersey. Plaintiffs presented scientific evidence from the world's leading computer science, computer security, and physical security experts that the State's DREs are critically unreliable and insecure. This insecurity threatens the most fundamental of our Constitutional rights; rights that are vigorously protected by statute and by the State's courts. Plaintiffs' witnesses conducted comprehensive scientific analyses of the Sequoia Advantage 9.00H, WinEDs System, and security seals. Their studies informed their conclusions that the entire voting infrastructure of the State can be readily attacked.

Plaintiffs' presented overwhelming evidence that the Defendants' voting machines are inaccurate, unreliable and insecure. In stark contrast, the Defendants' expert witnesses conducted no testing of the 9.00H DRE, WinEDS, or security seals. Indeed, Defendants' witnesses do not even possess the skill, expertise or experience needed to conduct similar scientific analysis.

Plaintiffs also demonstrated with overwhelming evidence that the Sequoia Advantage Version 9.00H has neither been certified nor thoroughly tested as required by N.J. Stat. Ann. §§ 19:48-1, 19:48-2, 19:53A-3 and § 19:53A-4. Again, in stark contrast, Defendants provided neither testimony nor documentary evidence to the contrary.

As such, it is incumbent upon this Court to enjoin the use of the Defendants' 9.00H DREs and to order the Defendants to replace them with auditable, secure voting systems with a proven track record. Precinct-based optical scan voting systems are supported by everyone in the scientific community, with the exception of Dr. Shamos. Most voters in the United States now use these voting machines. And, soon federal law may require that precinct-based optical scanners be used. Thus, this Court should order the Defendants to use the remaining $19 Million in HAVA funds to purchase those voting machines. Such an order is appropriate, as the Defendants have failed for five years to follow statutory mandates requiring auditable elections.

Additionally, the Court should order the Defendants to constitute a qualified group of experts to draft guidelines for evaluating computer-based voting systems. The Court should also require that the Title 19 Voting Machine Certification Committee be comprised of computer security experts who have the capability to "thoroughly test" voting machines, as required by law.

Respectfully submitted,

By:______________________________
Penny Venetis
Rutgers Constitutional Litigation Clinic
123 Washington Street
Newark, NJ 07102

By:______________________________
John McGahren
Caroline F. Bartlett
Patton Boggs, LLP
One Riverfront Plaza, 6th Floor
Newark, NJ 07102

Attorneys for Plaintiffs

DATED: July 2, 2009
Newark, NJ