FRANK ASKIN, Esq.
PENNY M. VENETIS, Esq.
RUTGERS CONSTITUTIONAL LITIGATION CLINIC
123 Washington Street
Newark, New Jersey 07102
(973) 353-5687
Attorneys for Plaintiffs

Assemblyman Reed Gusciora, Stephanie Harris, Coalition for Peace Action, and New Jersey Peace Action, Plaintiffs, v. James E. McGreevey, Governor of the State of New Jersey (in his official capacity) and Peter C. Harvey, Attorney General of the State of New Jersey (in his official capacity), Defendants.	SUPERIOR COURT LAW DIVISION MERCER COUNTY Docket No. **SUPPLEMENTAL CERTIFICATION OF ANDREW APPEL**

Andrew Appel, being of full age, hereby certifies:

1. None of the tests described in the Attorney General's Brief, the Certification of Patricia DiConstanzo, and Certifications of other election administrators are tests that will reveal whether or not the right software is installed in electronic voting machines, nor can the tests determine whether malicious software has been installed in DREs.

2. The DRE voting system safeguards and testing procedures described in the Attorney General's Brief and the Certifications of various election officials across the State do not address the problem of errors or fraud in the software itself. Many of the described safeguards are implemented by the software in the voting machine. An example of such a safeguard is having the machine print out a statement that it has not been tampered with since the functional test (pre-LAT test). (Def. Exhibit G, 14). Such a safeguard, since it is a statement made (in effect) by the software itself, will not be effective if software itself has been altered. Fraudulent software could easily misrepresent itself.

3. The statement of Abigail McCaw confuses "testing and certification," (Def. Exh. D., 3) but I will to refer to what she describes as "testing." Although this testing is useful to catch hardware malfunctions and inadvertent mistakes, none of the test she describes (Def. Exh. D., 5,7,11-17) are effective in determining what control software is actually loaded onto the machines, since these tests are mediated by that very software itself. Thus, the testing performed on and by iVotronic voting machine systems as described in the Certification of Abigail McCaw is not adequate to for determining whether the voting machines contain the correct software (or fraudulent software) and cannot detect latent flaws.

4. The certification sheet described in the Certification of Abigail McCaw is not an independent audit. (Def. Exh. D, 14). If there are flaws in the software of the machine, it may misrecord votes, and then to print a report which agrees with the votes misrecorded in the machine. As described in my previous testimony, bad software can cause machines to misrecord votes.

5. The tests described in the Certification of Patricia DiConstanzo (Def. Exhibit E, 10-17) are not adequate to detect the integrity and performance of the software installed within Sequoia Pacific AVC Advantage voting machines. The functional testing described is useful to detect burnt-out lightbulbs (or LEDs) and mechanical problems. Functional and diagnostic tests are not foolproof even to catch mechanical problems, and they should never be relied upon to catch fraudulent software.

6. The Certification of Patricia DiConstanzo notes the physical vulnerability of Sequoia Pacific AVC Advantage voting system. (Def. Exhibit E, 17). She explains that the there are two “tamper-proof” seals attached to the CPU board cover, and she asserts that if CPU board covers were removed and someone replaced the contents of the memory (or the memory chip itself) that contains the software, this would cause the protective counter to advance and would reinitialize the machine in the

“pre-LAT” mode. However, if fraudulent software were installed, such software could easily misrepresent the contents of the protective counter, and could reinitialize itself in any mode that the programmer chose. Thus, while she describes two layers of protection (tamper proof seals, then the state of the software), the second layer is not an effective protection fraudulent software. I have already discussed the inadequacy of seals in my first Certification (Certification of Andrew Appel, 52).

7. Fraudulent software would not reliably implement the safeguards described in the Certification of Patricia DiConstanzo. It is the software that tells poll workers that the machine is in the pre-LAT mode and software that tells you what the protective counter says. If software is altered, poll workders could be given false messages about the machine being in pre-LAT mode, or could be given a false reading of the protective counter.

8. The internal audit capacity of the DRE voting systems scheduled to be deployed in the upcoming election is not an independent audit. Defendants’ Brief and the Certifications of election officials, such as Patricia DiConstanzo, note that there is a random internal audit trail recorded by the machine which can be printed after the election. (Def. Exhibit E, 22). This

audit trail is constructed by the very software itself that should be independently audited. If fraudulent software is installed in a voting machine, it is likely to make the internal audit trail cover up whatever manipulations or miscalculations it has caused.

10. The physical vulnerability of DRE voting machines is made more problematic by the early delivery of these machines to polling places. The Certifications of various election officials indicate that DRE voting machines are delivered in advance of elections by private moving companies and, in some cases, by election officials themselves. The Certification of Mark Harris states that DRE voting machines are delivered to polling places "during the two weeks prior to the election" (Def. Exhibit G, 11). Although I would hope that in a typical polling place (such as an elementary school) the machines would be stored in a locked room, I would expect that election officials cannot have perfect control over access to rooms in elementary schools. During this advance period people could have unobserved access to the machines for several hours at a time. Machines could be tampered with, malicious software could be installed, and the protective seals could then be replaced.

11. The Certification of Mark Harris describes a print-out of vote totals that is made when the polls close. (Def. Exhibit G,

19). This will help detect only those errors that are made after the print out is complete. That is, if printed totals are produced, and then mistakes are made during the subsequent transmission of results from the voting machines, such errors could be detected. However, if the software makes (inadvertent or deliberate) mistakes between the time the voter casts the vote and the close of the polls, the print-out is not guaranteed to detect such an error.

13. The statements of Michael Frontera confirm that an independent audit is not contained with in the voting system, as the internal audit report is generated from the same potentially flawed software used to record votes. (Def. Exhibit P, 6c.)

14. Although Michael Frontera states that the auditability of DRE machines is superior to that of lever machines and of paper ballots, (Def. Exhibit P, 6c) it is not at all clear that this is true. Clearly, paper ballots have marks that the voter herself can write and read, so there need be no unauditable software between the voter and the ballot, or between the ballot and the persons conducting a recount. Lever machines, although not immune to malfunctions or to fraud, tend to produce evidence of another kind when such problems occur: an undervote. That is, by the nature of the machines' design, it is difficult to rig a lever machine to transfer votes from one candidate to another;

what happens instead is a failure to record some votes. When the vote total for an office is significantly less than the number of voters, this is an indication (but not proof) of a problem. This is an undesirable situation, of course. But a worse problem would be election fraud which goes undetected because there is neither an overvote nor an undervote. This is the type of fraud that could be committed by manipulating DREs. Fraud or miscalculation on DRE voting systems does not necessarily result in an undervote.

15. Michael Frontera (Exhibit P, 6d) confuses two statements I made in my Certification. I said that new software could be loaded into the Sequoia AVC Edge by inserting a smart card and typing a password, a process that might take as little as five minutes. (Cert. Of Andrew Appel, 50.) I further said that to insert new software in the Sequoia AVC Advantage is more complicated: one would need to replace a memory chip and replace a seal, and this process would take “at least ten minutes of unobserved access to the machine.” (Cert. of Andrew Appel, 53) Mr. Frontera does not dispute my statement about the AVC Edge. He does not dispute the substance of my statement about the AVC Advantage, except to add that in addition to the seals, there are keyed locks and “at least ten screws” (Def. Exhibit P, 6d). These statements are consistent with my statement that it would take at least 10 minutes to replace a memory chip within a

machine. I did not suggest, as Mr. Frontera claims (Def. Exhibit P, 7) that this could be done in 10 minutes in front of poll workers; I said, “at least 10 minutes of unobserved access to the machine.” These machines are thus vulnerable at any points in their lifetime when people have unobserved access to them for periods of hours.

_____

Andrew W. Appel

Dated: October 25, 2004

Princeton Township, New Jersey