Princeton University **Department of Computer Science**
35 Olden Street
Princeton, New Jersey 08540-5233
Tel: (609) 258-4627 Fax: (609) 258-4771
appel@princeton.edu

Andrew W. Appel
Professor

May 27, 2008

Richard Woodbridge, Esq.
Chair, New Jersey State Voting Machine Examination Committee

Dear Mr. Woodbridge:

I would like to thank you for conducting the public hearing of May 22, 2008 in such an open manner. At that hearing I raised one issue (concerning verification of the emptiness of the ballot bag); in addition, because I had to leave early to attend another obligation, Professor Penny Venetis of Rutgers Law School spoke on another issue on my behalf (concerning Flash memory). In this letter I would like to explain both of these issues, as well as a third issue (concerning ballot serial numbers).

First, on the ballot bag. An important safeguard in elections that use paper ballots is that board workers (also called poll workers) and poll watchers (also called challengers) can witness the fact that the ballot box is empty immediately before the opening of the polls. On the Seqouia AVC Advantage D10 DRE machine exhibited at the hearing on May 22, there is a ballot bag instead of a ballot box. Election officials of the State of New Jersey, when specifying procedures to be used in connection with voter-verified paper record systems (VVPRS) may wish to institute an explicit step of permitting challengers and board workers to see for themselves that the ballot bag is empty. However, it is not at all obvious that the physical design of the ballot bag permits this.

The ballot bag has a small slot on the top, which is intended to be connected to the output of the VVPRS printer; and it has a zipper at the bottom, which is to be used for removing the paper ballots after an election. The zipper opening is locked with a key.

Mr. Winham from Sequoia told me on May 22 that the intention of the designers is that the zipper key will never be present in the polling place, and that the zipper opening is to remain sealed shut until the ballot bag is delivered back from the polling place. Of course, the specification of these procedures is at the discretion of State election officials, but these precautions seem reasonable in general. Thus, at the beginning of an election day, when board workers (observed by challengers) are setting up the voting machine, the (presumably empty) ballot bag is removed from the inside of the voting machine, and attached to the printer on the outside of the voting machine, and during all this time the zipper is locked shut.

During this process it is not clear how board workers and challengers can observe whether the ballot bag is empty. Perhaps they can do so, visually, through the narrow slot at the top of the bag, or they can do so by shaking the bag, or both. It is not obvious to me that such procedures would be effective. I believe it would be useful to come to some conclusions on this issue before certifying the printer attachment for use in New Jersey elections.

Second, the issue of flash memory in the AVC Advantage D10. As you know, after a voting machine has been certified by the Attorney General (or now, by the Secretary of State) pursuant to New Jersey law, any subsequent modification to the machine that does not "impair the accuracy" of the machine shall not require a new certification. In your hearing of May 22, you invoked this clause, and therefore held a hearing only to certify the new printer attachment, and did not hold a full certification hearing on the AVC Advantage D10 voting machine.

As I will explain, the internal design of the AVC Advantage D10 is a very substantial modification of the earlier AVC Advantage voting machine. This redesign contains a specific feature, the use of flash memory to hold the voting-machine control software, that does impair the security, and therefore the accuracy, of the voting machine. Therefore, I believe it is appropriate to hold a full certification hearing, and it is not appropriate to invoke the "does not impair the accuracy" clause.

Older-model AVC Advantage voting machines held the control program (known as "firmware") in a read-only memory (ROM). Sequoia, in its document entitled "AVC Advantage Security Overview" (2004) claimed that this means that it is impossible to load a new voting-control program from the Ballot Cartridge (a.k.a. Results Cartridge). Specifically, Sequoia claimed,

"This ROM contains the AVC program instructions, or firmware. The ROMs cannot be changed without removal from the system ... The design of the ... electronics of the AVC do not physically allow data to be read from ... RAM and executed as instructions... Hence, no data in the AVC RAM could be executed as an instruction." (p. 13.)

Although I have not had the opportunity to scientifically verify these specific claims, they are plausible claims, and for the purposes of this discussion I will rely on them.

RAM refers to "random-access memory", that is, memory that is writable as well as readable. Both the internal circuit board and the removable Ballot Cartridge contain RAM. It is very important that hackers should not be able to change the program that adds up the votes simply by inserting ballot cartridges. Therefore the safeguard that Sequoia built into their older-model Advantages was an important one. It meant that, in principle, one could not replace the firmware without physical access to the voting machine, i.e. without opening up the voting machine and physically replace ROM chips.

The newer model AVC Advantage D10 that was demonstrated on May 22 lacks this important safeguard. According to the report by Wyle Laboratories on the D10, dated July 26, 2007,

"[The] Main CPU ... contains 8 Mb of DRAM, 2 Mb of Flash ROM (used for application program storage, ballot definition, and vote data storage), a PCMCIA slot (used for the results cartridge), [etc.]"

At the public hearing on May 22, Professor Venetis asked whether this description was accurate, and received the answer that it was.

The "application program" referred to by Wyle's report is, in fact, software that records votes, interacts with disabled voters through the "audio kit," and prints VVPRS papers.

The replacement of this software by criminal means could lead to election fraud. "Flash ROM" is a technology that is in some ways like ROM (that it does not "forget" when electrical power is removed) and in some ways like RAM (that new data can be written into it by the computer it is attached to, without removing it from the circuit board, entirely under the control of the computer program that is running).

In recent years, scientists have had the opportunity to study other models of voting machines that store their control software on flash memory: specially, the Diebold AccuVote-TSx, the Sequoia AVC Edge, and the ES&S iVotronic. (Studies commissioned in 2007 by the Secretaries of State of California and Ohio; I attach relevant citations and excerpts as Exhibit A.) In every case, it was found that fraudulently prepared ballot cartridges, when inserted in the voting machine, could cause a new (fraudulent) control program to be copied into the flash memory. Furthermore, the new control program could even be designed to write a copy of itself to any other ballot cartridge ever inserted into the machine. These other ballot cartridges would then be vectors for the viral propagation of fraudulent vote-stealing software.

Storing the voting-machine control program on flash memory is a design risk. Every voting machine with this design that has ever been studied by independent security experts, including one machine from Sequoia, has failed to mitigate this risk, and permits viral propagation of fraudulent software, *without the attacker ever having physical access to any voting machine.* The change made to the AVC Advantage design, leading to the D10 model, does "impair its accuracy." Therefore I urge you to hold a full certification hearing of this machine.

Third, serial numbers are printed on the ballot. Just before the meeting on May 22 I had an opportunity to cast votes on the machine in the hearing room, and I was given the paper VVPRS ballots resulting. I attach a copy of the printout (labeled "Exhibit B"). A 5-digit serial number is printed on this ballot, once at the top and once at the bottom.

One of the safeguards that has been customary for over a century with paper ballots is to preserve the secrecy (privacy) of the ballot. This means not only that only the voter should know how he or she voted, but that the even with the cooperation of the voter, another person cannot learn how he or she voted. In short, it must be the case that the voter cannot prove to another person how he or she voted, even voluntary. This is necessary to avoid both vote-buying and voter coercion.

I was told on May 22 by a representative of Sequoia that the serial number printed on the ballot corresponds to the same serial number on an internal electronic "ballot image." A five-digit serial number is easy for a voter to remember or to write down. These serial numbers will be visible during a recount or an audit, and since they will in any be present in the ballot images in the Results Cartridge from the voting machine. Thus it may be possible for a voter to use this number to prove how he or she voted; this in turn opens to door to vote-buying and coercion.

Thus there is a reasonable and legitimate question of whether this voting machine in its present form provides for a truly secret ballot. I believe it would be useful to explicitly consider this issue before certifying the printer attachment for use in New Jersey elections.

Sincerely,

Andrew W. Appel
Professor of Computer Science

Exhibit A.

Citations regarding the viral propagation of fraudulent vote-stealing software on voting machines whose control programs are stored in flash memory. Note that the AVC Advantage D10 was not studied in either study, as it was not at that time certified for use in either CA or OH.

California Top-to-bottom study, commissioned by Secretary of State Debra Bowen (2007).

"Source Code Review of the Diebold Voting System", by Joseph A. Calandrino *et al.* July 20, 2007.
http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf, fetched May 27, 2008.

Section 3.1 explains how the Diebold (now called Premier) AccuVote is susceptible to this problem.

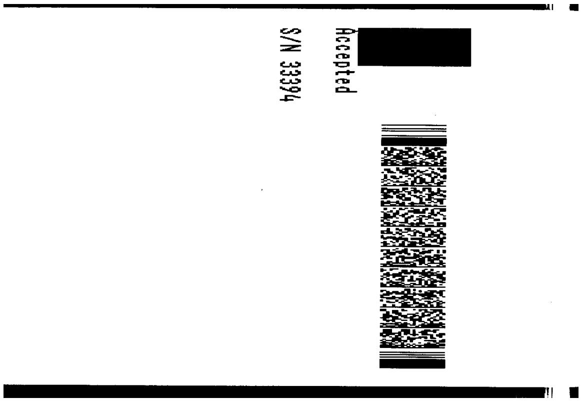
"Source Code Review of the Sequoia Voting System", by Matt Blaze *et al.*, July 20, 2007.
http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf, fetched May 27, 2008.
Section 3.1.2 (and others) explain how the Sequoia AVC Edge susceptible to this problem.

Ohio EVEREST study, commissioned by Secretary of State Jennifer Brunner (2007).

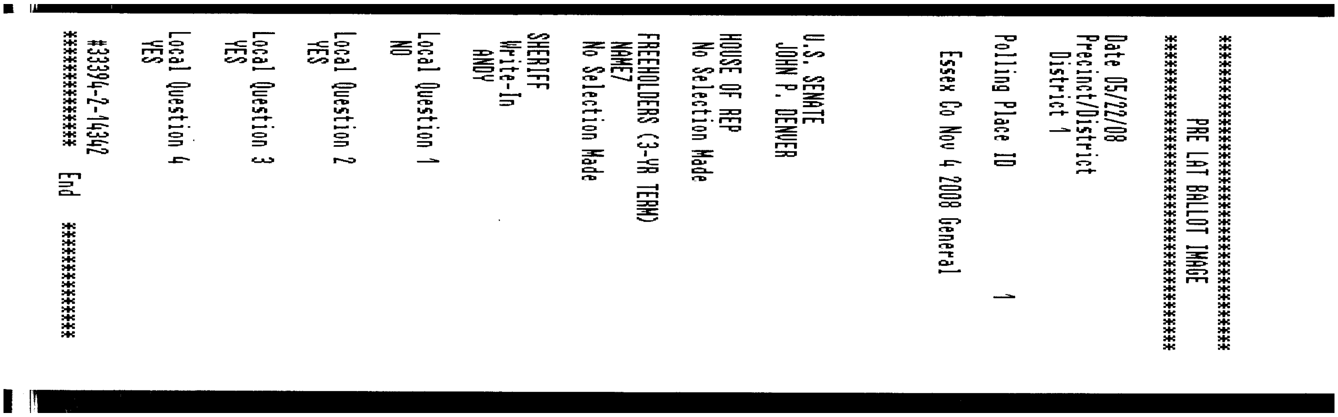
"EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing, Final Report", December 7, 2007.
http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf
(fetched May 27, 2008)

Section 6.3.1 explains how the ES&S iVotronic is susceptible to this problem. Section 12.3.1 explains how the Diebold (now called Premier) AccuVote is susceptible to this problem.

Exhibit B. Copy of a voter-verified paper ballot from an AVC Advantage D10 voting machine, produced May 22, 2008.
First image is the top of the ballot, with bar code and serial number.
Second image is the bottom of the ballot, with serial number repeated just before *** End ***



```
[redacted]
Accepted
S/N 33394
```



```
****************************
    PRE LAT BALLOT IMAGE
**************************
Date 05/22/08
Precinct/District
  District 1

Polling Place ID            1

  Essex Co Nov 4 2008 General

U.S. SENATE
 JOHN P. DENVER

HOUSE OF REP
 No Selection Made
FREEHOLDERS (3-YR TERM)
 NAME7
 No Selection Made
SHERIFF
 Write-In
  ANDY

Local Question 1
 NO

Local Question 2
 YES

Local Question 3
 YES

Local Question 4
 YES
  #33394-2-14342
************  End  ************
```