



**October 2, 2008**

## **RESPONSE FROM SEQUOIA VOTING SYSTEMS TO THE EXPERT REPORT OF ANDREW W. APPEL EVALUATING THE SECURITY AND ACCURACY OF THE SEQUOIA AVC ADVANTAGE DRE VOTING COMPUTER**

*In The Matter Of Assemblyman Reed Gusciora, Stephanie Harris, Coalition For Peace Action, And New Jersey Peace Action, Plaintiffs V. Jon Corzine, Governor Of The State Of New Jersey (In His Official Capacity) And Anne Milgram, Attorney General Of The State Of New Jersey (In Her Official Capacity), Defendants*

### **EXECUTIVE SUMMARY**

Sequoia Voting Systems is presenting this report in response to the Expert Report of Andrew W. Appel Evaluating The Security and Accuracy of the Sequoia AVC Advantage DRE Voting Computer report (“academics’ report”) produced by Andrew W. Appel and his associates (“the academics”) in relation to: The Matter Of Assemblyman Reed Gusciora, Stephanie Harris, Coalition For Peace Action, And New Jersey Peace Action, Plaintiffs V. Jon Corzine, Governor Of The State Of New Jersey (In His Official Capacity) And Anne Milgram, Attorney General Of The State Of New Jersey (In Her Official Capacity), Defendants.

Sequoia Voting Systems is a leading provider of election technology and has been serving its state and local government customers throughout the United States for over 100 years. Sequoia currently provides voting equipment to jurisdictions in 17 states plus the District of Columbia.

The purpose of this report is to provide a response to the Plaintiff’s report in a lawsuit against the State of New Jersey regarding voting equipment. The lawsuit alleges that the voting machines used for years in the majority of New Jersey counties are inaccurate, insecure, and unreliable – and thus unconstitutional for use in New Jersey.

Nothing could be further from the truth. The Advantage voting machine has been in use successfully since 1987 and provides accurate results.

Through this report response, we will show how simple, established, and previously used accuracy and security protections, removed from the units studied in the report published by the Plaintiffs, make the items in the academics' report and accompanying video next to impossible. Many of the scenarios painted by the academics hired by the Plaintiffs depend on the existence of crooked, malicious, and corrupt pollworkers. The success of some scenarios depends on BOTH corrupt pollworkers and inattentive voters.

Throughout our report, we have debunked some of the academics' theories around how to manipulate an Advantage voting machine. As with similar past studies on election equipment, although made to look like a real election, this study is conducted in a laboratory. The machines the academics tested had factory security hardware removed, specifically the security screw that protects the computer chips containing the vote counting software. Similarly, the academics must have forgotten about the plastic operator panel cover, although one of their colleagues wrote about in his blog after seeing it in use on an Advantage voting machine during a New Jersey election several months ago. These two simple, established protections, as well as keeping the election computers off the Internet, render the attacks discussed in the academics' report and accompanying video far less sensational and more importantly far, far less likely to succeed before they are stopped, or at minimum, detected. Tampering with voting machines is a State and Federal crime with both fines and prison time as part of the sentence. All of these items need to be taken into consideration when examining voting equipment because election security is all about the people, processes and voting technology, not just the voting technology in an isolated, sterile classroom environment.

In particular, we take the academics to task for their inflammatory tone – using “steal” over 100 times, their editorializing on the wonders of paper ballots and optical scanning, their numerous factual errors and cases of intellectual dishonesty (several of which we will highlight), and their inappropriate and uninformed extrapolations to versions of the AVC Advantage that were not studied.

There have never been any documented instances of fraud being carried out on the Advantage, on any other Sequoia machine or on any other company's electronic voting equipment in a live election in the United States. Any issues related to election results on Sequoia Voting Systems equipment have been investigated by the jurisdiction and Sequoia; and concrete, attributable causes other than fraud have been found for each. Post-election audits, contrary to the assertions in the academics' report, have and will continue to successfully bring to resolution any actual or perceived election results discrepancy.

There are some good and useful areas for improvement of both the Advantage specifically, and election security in general, that can be drawn from the academics'

report. These points in the report drive home the concept that any election security-related items can be mitigated with procedural protections, many of which are already established across the United States and of course in New Jersey. Sequoia has listened to the concerns of election officials throughout the nation and developed enhanced security measures that are in place in its latest product offerings. These offerings are currently undergoing both Federal Certification and New Jersey State Certification. Some jurisdictions have in fact already deployed these new products.

## **INAPPROPRIATE STANDARDS**

Throughout their report, the academics evaluate the AVC Advantage against inappropriate standards.

For example, the academics declare that the Advantage “must be correct in all circumstances”, without explaining that nothing can meet this standard - not mechanical systems, not electronic systems, not software systems, and not human systems. Yet they go on to assert that in a paper-based voting system, “it suffices to recount the paper by hand”. They are apparently ignorant of the decades of fraud and vote stealing chicanery that voting machines, beginning with lever machines, were deployed against.

In another example, seen in dozens of places in the academics’ report, they hold the Advantage to the 2002 VSS and sometimes the 2005 VVSG, knowing full well that these standards did not exist when the version they reviewed was developed. In fact, New Jersey does not require Federal Certification. The State does; however, require approval from a federally accredited voting system test laboratory prior to scheduling a Technical Review Committee (also known as the Title 19 Committee) Hearing.

## **THE EXPERT REPORT**

The team reviewing the report produced by the academics noticed numerous areas of factual inaccuracy, faulty extrapolations, bias, and editorializing in the academics’ report. Following are some specific rebuttals; however, this is not a comprehensive list.

### Section 2.5

In the second bullet of Section 2.5, the academics’ report states the following: “Second, it writes these [cast vote] totals (along with a record of the votes cast in each ballot, the “ballot image”) to a Results Cartridge, about the size of a VCR tape, that is then removed from the voting machine.” This statement is incorrect. Vote data is written to the Results Cartridge after each voter, and at all times the internal memory and Results Cartridge storage must be identical or the machine will halt. Writing the votes simultaneously to their being cast is far more reliable than the machine operation falsely conjectured by the academics’ report.

## Section 2.7

In Section 2.7, the academics' report states the following: "Therefore it is absolutely crucial that the firmware should be correct in all circumstances, and the voting-machine firmware should be immune to tampering. But this is not the case." In addition, the footnote to Section 2.6 states the following: "Thus, a DRE cannot be effectively audited. In contrast, an optical-scan voting machine *can* be audited in a way that is truly independent of any computer program that might be suspected of cheating. An optical-scan voting machine works as follows: the voter fills in a paper ballot by using a pencil to fill in circles or ovals next to the name of the candidates she wishes to vote for. Then, (in "precinct-count optical-scan") she takes the ballot to the optical-scan machine, and feeds the ballot through. The machine counts her votes, then drops her ballot into a ballot box. To audit an optical scan voting machine, it suffices to recount the paper ballots by hand. This method does not work with DREs that have no paper ballot."

The term "correct in all circumstances" in Section 2.7 plus the footnote to 2.6 show rather clearly the bias towards paper ballots apparently held by the academics. They desire to hold DRE machines to an impossible standard, while suggesting that optical scan audits consist of nothing more than hand-counting the scanned ballots. This is clearly not the case. For an extensive overview of the complexities of working with optical scan ballots and the intricacies of conducting audits of optical scan elections, please see a research paper on this topic titled "The New Mexico 2006 Post Election Audit Report" by Lonna Rae Atkeson (University of New Mexico), R. Michael Alvarez (Caltech) and Thad E. Hall (University of Utah) that was issued on September 22, 2008.<sup>1</sup> A visual overview of these researchers' experience with paper ballots can be found on the Election Updates blog at <http://electionupdates.caltech.edu/?p=1814>.

## Section 5

Throughout Section 5, the academics speak to the ease of which they could replace the computer program chips (aka ROMs or firmware). The academics fail to mention that either prior to or during their testing that the factory-installed security screw and seal were removed. The removal of these pieces of security hardware renders the academics' conclusions of installing fraudulent firmware null and void.

---

<sup>1</sup> The report is available at [http://www.pewcenteronthestates.org/uploadedFiles/wwwpewcenteronthestatesorg/Reports/Electionline\\_Reports/electionlineWeekly09.25.08.pdf](http://www.pewcenteronthestates.org/uploadedFiles/wwwpewcenteronthestatesorg/Reports/Electionline_Reports/electionlineWeekly09.25.08.pdf)



***Figure 1: Security Screw - installed, with security cap which deters removal and prevents undetected removal***



**Figure 2: Serial-numbered crimped metal CPU security seal**

### Section 5.7

In Sections 5.7 and 10.12, the academics mischaracterize a plastic strap seal on the Results Cartridge socket as providing “tamper evidence if the circuit board cover is removed” and then go on to state that this seal is ineffective at detecting circuit board cover removal. The referenced plastic strap seal is obviously intended only to evidence unauthorized removal of the Results Cartridge and to assert otherwise shows a lack of rigor by the academic team and misleads the reader.

### Section 10.6

In Section 10.6, the academics give a list of five (5) aspects that would lead to a secure tamper-evident seal program. They claim that none of these five are “true in practice”. Let us review at these items.

For the first aspect in this bulleted list, the machines that the academics examined had their security screw and CPU seal removed from the unit prior to or during the testing invalidating their “conclusions” regarding Advantage security.

In relation to the second aspect, they say that plastic seals can be easily defeated. Neither the report nor the accompanying video shows a plastic seal being defeated except of course for the farcical bit where the cartridge seal is claimed to be the CPU

cover seal – which it is not, see above and Sections 5.7 and 10.12 of the academics’ report).

In relation to the third aspect, please see the response noted in response to the first aspect above. These seals are never meant to be removed except in cases of legitimate repair to the CPU board, which is a rare occurrence.

In relation to the fourth aspect, the academics say that seals can be substituted because the serial numbers are not routinely logged. This is not a failure of the AVC Advantage, but a State and County procedural issue that is equally valid for every voting system that has ever been created.

In relation to the fifth aspect, the State of New Jersey has indeed made sure that custom printed serialized tamper-evident seals are available throughout the State and have provided instructions for their use to all counties, rendering this point erroneous.



### TECHNICIAN'S INSTRUCTIONS ALL MACHINES

Security Screw Cap (upper left hand corner) Insert screw into back of cap. Place numbered cap over screw. **Record number.**

Numbered wire seal (upper right hand corner) Insert numbered wire seal. Lock seal and remove excess wire. **Record number.**

Results cartridge seal – Insert plastic numbered seal. **Record number.**

### AUDIO MACHINES

#### ***Tamper evident tape (3 pieces)***

1. Left hand side-place a piece of tamper evident tape from the e-box to the metal shroud horizontally.
2. Place tamper evident tape horizontally from metal shroud to side of audio box.
3. Place tamper evident tape over audio cartridge and onto audio box vertically. **Record number.**

### NON-AUDIO MACHINES

#### ***Tamper evident tape (1 piece)***

Left hand side- place a piece of tamper evident tape from the e-box to the metal shroud horizontally.

**Figure 3: New Jersey's instructions for proper sealing of the AVC Advantage.**

Conclusion: The academics have not kept up with current local and nationwide developments in election security or for some reason have chosen to leave these

developments out of their report. There are several other instances (See Sections 14, 15, and 22 for a few of these) in the academics' report where currently utilized election security practices are ignored, leading to faulty conclusions in that report.

### Section 11

Throughout Section 11, the academics detail how they could theoretically reverse-engineer the firmware of the Advantage. Significantly, they fail to mention that they cannot put the reverse-engineered code back into the Advantage or how they would do this after describing in great detail how they could reverse-engineer the firmware. Without a method for successfully re-installing the reverse-engineered firmware, this reverse engineering exercise is a waste of time. During the investigation/classroom experiment that produced their report, the academics relied on compilers and other tools provided by Sequoia. It took Sequoia (the Advantage developer and manufacturer) engineers two weeks to make ready and provide these tools to the academics. The academics' also failed to account for new product introductions by Sequoia. New voting machine software is typically introduced to the marketplace every year or two. New voting machine firmware would lay waste to any ongoing reverse-engineering program for two reasons:

1. The installation of new voting machine software (also known as firmware) cleans out any old firmware, so if by some extremely slim chance a reverse-engineered firmware is present on the voting machines, it would be removed and replaced by the new and correct firmware; and
2. New manufacturer's firmware is just that – new. The new data structures and software code would require that anyone attempting to reverse-engineer the firmware re-start some portion of their efforts to match the new firmware, that is, assuming they could get a copy of that new firmware which is kept behind the various security locks and seals on the voting machines.

In short, all of the fanfare around reverse-engineering of firmware is at best misleading since the academics offer no method to actually put a reverse-engineered firmware into a voting machine or to keep up with new firmware introductions from Sequoia.

### Section 11.11

In Section 11.11, the report on the "simulator", a software program that allows analysis of the Advantage firmware on a personal computer, indicates it is far from the complete and wondrous tool the academics describe.

For example:

- "Because the Advantage's mechanism for reading user input is to set a bit when a button is pushed and to clear that bit when the button is released, there is an incompatibility between Swing's basic event model, and the requirements of accurately simulating the Advantage."
- "In timing tests, the simulator has performed reasonably well, approaching real-time performance with speeds of about 4 MHz when run without the front-end."

In other words, WITHOUT the user interface components. That's hardly a useful tool.

And most telling:

"One current shortcoming of the simulator is that when executing the Advantage's firmware, the simulator eventually halts because portions of the Advantage's firmware are only executed in response to raised interrupts and the simulator does not yet implement the recently reverse-engineered interrupt controller."

So, the academics' claim of simulating the Advantage in three man-weeks is egregiously intellectually dishonest.

Also from the simulator report:

"One improvement would be to modify the GUI so that it more closely resembles the interface of the actual Advantage."

Isn't that what a reasonable person would expect a simulator to be doing?

### Section 12

Section 12 is rendered moot when the proper CPU cover seals are installed because the fraudulent replacement of the microprocessor in the Advantage is either deterred or detected by these seals. Also, it does not pass the common sense test that an army of hackers could:

- visit all or most of the over 10,000 Advantage voting machines in New Jersey
- carry in un-noticed the bulky desoldering tool in figure 18 of the academics' report
- remove the security seals and screws on the voting machines,
- desolder, remove, and replace the microprocessors;
- make sure the now faked Advantage actually works, and then
- put all of the sheetmetal and security devices back in place without providing evidence of their crime and without damaging the Advantage.

### Section 12.14

In Section 12.14, the academics continue to state that fake processor chips are a "threat". That is, at this time, as implied throughout this section, a fake Advantage processor does not exist. Sequoia's surveillance likewise has not detected any fake processor chips that would be suitable to cause an Advantage to malfunction. Frankly, this entire section is a fantasy.

### Section 14

Section 14, which attempts to state that there is no verifiable means to check voting machine firmware, is also completely off the mark. It does not reflect current security practices. For example, the State of Nevada is using widely available third party

software to perform pre and post-election firmware validation. Contrary to the academics' report in Sections 14.6 and 14.7, the third party validation software can be procured by interested citizens thus enabling them to participate (under the supervision of the State) in the firmware validation process. This validation can be performed on known clean PCs mitigating the concerns in Section 14.7. Similarly, it would be a simple matter to physically disable any ROM testing device's ability to write to the ROM chips. This would add protection beyond the requirement to erase the ROM before writing to it, a process that uses a special ultraviolet light source and takes 10-15 minutes.

### Section 15.3

In Section 15.3, the academics state the following: "In general, we should assume and believe that the people who run our elections are honest." Sequoia agrees with this. In this light, regardless of election technology employed (hand counted paper ballots, optical scan, DREs or lever machines), there are always a large number of insiders who must be trusted. Conducting elections – no matter the voting system – is a people-based process. The obvious bias of the academics toward optical scan voting systems thus has no place in a report to the Courts of New Jersey.

### Section 16

Section 16 speaks to software independence; a concept first brought light in 2006, years after the development and initial certification of the Advantage voting machine. Sequoia developed the Voter Verifiable Paper Audit Trail (VVPAT or VVPRS in New Jersey statute). The State of Nevada utilized VVPATs in their 2004 General Election, which represented the first widespread use of VVPAT technology. The use of VVPAT meets the EAC's definition of software independence. It is important to note that the model of the Advantage recently successfully tested by the New Jersey Institute of Technology and currently under consideration for New Jersey State Certification contains a VVPAT.

### Section 17

In Section 17, the academics state that manipulating the firmware in an Advantage is "straightforward". This claim is opposed by the fact that the voting machines they tested did not contain either factory installed or State mandated security screws and seals. The academics fail to mention that their experiments required significant effort from Sequoia, the manufacturer, to provide the team of graduate level computer scientists with the needed build tools and compilers to make their experiments possible.

### Section 18

In Section 18, the academics continue to make exaggerated claims regarding security issues with the Advantage. Sequoia has never represented that the 9.00 Advantage meets either the 2002 VSS or 2005 VVSG. The Advantage 9 was certified to the 1990 Federal Voting Systems Standards, which do not contain the requirements referenced in this section of the academics' report. The academics also misunderstand the context of the requirement in the 2002 and 2005 standards. Throughout these standards, and even in the 1990 version, "election-specific programming" is specifying logic elements

that change from election to election; what Sequoia calls the ballot definition (and implements solely as data files). It is the case that historically, including Sequoia's own Insight precinct optical scanner, that the election-specific logic was implemented as programming instructions, in other words "election-specific programming". It is improper to apply the term "election-specific programming" to the generic firmware that makes the hardware act as a voting machine, and which in the context of the 2002 and 2005 standards is more reasonably called the "operating system".

### Sections 21, 22, 23

In Sections 21, 22, and 23, the academics make numerous claims and process descriptions surrounding a virus infestation of the Advantage and/or the computers at election offices. These computers typically run WinEDS, which is the Sequoia Election Management System. An Election Management System helps the jurisdiction manage the election workflow from ballot definition to accumulation and reporting of results. The virus described in Section 21 can only lead to a denial of service attack on the Advantage audio subsystem. This also applies to the attack on the audio subsystem described in Section 26.2. Neither attack can "infect" the main systems of the Advantage through the audio board. Such a virus can, as the academics note, cause a power up "Audio Subsystem Not Found" error, but it cannot (and the academics do not claim such) do further harm. Viruses described in Section 21.8 would only infect machines being used for audio. Audio-equipped machines not being used for audio would not be infected. Any infected audio cartridge would not be inserted in this set of voting machines.

Section 22.8 describes the autorun feature of Windows as a means to propagate viruses onto WinEDS computers. In both the State of Colorado and the State of California, this feature of Windows is disabled before WinEDS computers are first used in election preparation. Similarly, these States and others disallow connections to the Internet by WinEDS computers. Sequoia concurs with these requirements and various Sequoia technical publications describe these protections and many others to prevent viral propagation amongst election computers and the voting machines. The academics attempt to denigrate these numerous safeguards by misinterpreting Section 23.13 "This Guideline provides only a portion of the information needed to fully protect the jurisdiction's election computing infrastructure". This sentence, accurately interpreted, states that election computer security goes beyond hardening the computers, to include organizational policies, personnel access safeguards, configuration control over the computers, and many other items. These computer hardening items have been used in elections in at least two states, after being installed by County IT persons with varying levels of assistance from Sequoia; and thus Sections 23.10, 23.11, and 23.14 are exaggerations made by the academics that could easily mislead the reader.

The academics also fail to point out safeguards currently in use in the United States which would stop any viral infestation and in fact eliminate it from the WinEDS computers. This includes the practice of reloading WinEDS from a clean copy just before each election cycle, so that if a virus did infect a WinEDS computer, it would be

removed and any malicious software likewise removed when the computer was reloaded with the fresh copy of Windows and WinEDS. This process requires less than four hours per election cycle in a medium-sized county.

In short, the headline above Section 23.9 “It is extremely difficult to truly secure the WinEDS computers” is a sensational attempt to mislead the reader.

In addition to their ignorance of modern election security techniques, Section 24.5 shows ignorance of New Jersey statute. New Jersey law requires emergency paper ballots be provided to each polling location in the event of issues with the voting machines. This law has been in place for many years. With emergency paper ballots at the polling place, the long lines envisioned by the academics simply will not materialize.

In Section 23.3, the footnote says “VVS”. Sequoia believes this should be either “VSS” if the academics refer to the 2002 Voting System Standards or “VVSG” if referring to 2005 Voluntary Voting System Guidelines. Sequoia has traditionally, and currently, recommends strongly that any and all election related computers are never connected to the internet or used for non-election purposes in any manner. It is of interest that Hanna-Barbara software is present on the WinEDS laptop purported by the academics to be the property of Union County, New Jersey.

The academics fail to mention that the version of WinEDS studied in the California Top to Bottom Review of 2007 is WinEDS version 3.1.012. This version is two generations prior to the version of WinEDS currently in use in New Jersey, which is WinEDS 3.1.074 (there was a 3.1.038 that was Federally Certified in between 3.1.012 and 3.1.074). Version 074 has not been reviewed by the California Secretary of State.

### Section 29.3

In Section 29.3 of the academics’ report, a few significant items are ignored or dismissed. First, the so called “barely audible chirping sound” is actually emitted by the Advantage at a sound level of 66 dB, well above the level of conversational speech, which hovers around 40 dB. Second, the booth light is NOT fluorescent, which should have been readily apparent in a rigorous examination. Third, the academics state that at least one county enables the lighting under the contest name. This lighting helps guide the voter, especially in a Primary Election where both Democratic Party and Republican Party candidates are shown on the ballot. Instead of calling for all counties to configure the Advantage system to light the contest names, the academics choose to criticize the voting machine for providing specific ballot presentation options and flexibility demanded by customers.

### Section 30

Section 30 falsely attributes various machine features and voter behaviors to the denigration of the Advantage. Section 30.4 inaccurately ascribes a one percent lost vote (a misnomer in and of itself) rate to the Advantage user interface. With all voting technologies there is an opportunity for a voter to enter the voting process but not cast a

ballot. On any DRE device, a voter may make selections but leave the DRE prior to pressing CAST VOTE or otherwise completing the act of casting a ballot. Similarly, voters leave paper ballots in the small booths allotted for voters to complete their ballot marking, and without actually placing their ballot in a ballot box for later tabulation. It is saddening that some percentage of voters do not complete the act of casting their ballot, but this is not due to DRE technology or the user interface of the Advantage. In the remainder of Section 30, the academics continue the story of the Advantage user interface misleading voters. However, they fail to mention that if the machine is not activated, there are significantly different behaviors by the machine from an activated machine:

- The booth light does not illuminate
- The CAST VOTE light does not illuminate after the voter makes his or her first selection
- The LCD panel does not show the Party activation (DEM or REP) when the voter enters the booth
- The “Vote Recorded, Thank You” message is present when the voter enters the booth
- The lights under the contest header and the selected candidates do not stay lit after a one second interval
- The 66 dB series of musical notes (aka the aforementioned derogatorily described “chirping sound”) is not played at either voter activation or when the CAST VOTE button is pressed
- For visually impaired voters using audio, the audio ballot does not play

These substantive omissions from the academics’ report render this section moot and misleading to the reader. At any rate, simple instructions to the voter, added to the existing instructions to the voter that all counties print on the ballot face, would mitigate any fears of voter disenfranchisement due to these so called shortcomings of the Advantage user interface.

### Section 31

Section 31 of the academics’ report is rendered moot by the plastic cover (shield) present on the Operator Panel since the February 2008 Primary Election. This cover prevents, even with repeated and forceful presses, extraneous button presses. The academics’ scenario in this section is thus a non-starter. In addition, the booth light turns off when the extraneous button is pressed. So, if a pollworker removes the operator panel cover, there continues to be a noticeable indicator to the voter. Finally, if a corrupt pollworker failed to activate a number of voters, the public counter (the counter that tells people how many voters have voted on the machine and is displayed for witnesses to view throughout Election Day) would not balance with the precinct pollbooks. In other words, the higher number of voting authority slips handed to voters than votes cast would cause suspicion. Similarly, there are multiple pollworkers in a polling location, so the opportunity for fraud is reduced as fraud would require a conspiracy among private citizen volunteer pollworkers to violate State law.

### Section 32.1

In Section 32.1 the academics fail to define what “too quiet” means. This is subjective terminology rather than a scientifically specific word. There should be no place in the academics’ report for subjectivity. The sound level on the activation sound is 66 dB, well above the sound level of conversational speech and easily heard by persons of average hearing, even with a level of background noise. Similarly in Section 32.4, the academics do not compare and contrast “fairly loud” with “too quiet” in specific engineering terms. As lever machines were last used in New Jersey circa 1987, it is interesting to note that the academics recall the sound level and quality emitted by those long since replaced voting machines. Section 32.6 continues this faulty line of reasoning. Pollworkers normally sit next to the operator panel since that is a geographic place where the task of voter activation is performed. The audible sound is therefore easily heard even over harsh background noise. The academics also contradict themselves in this section. How can a polling place have a “cacophony of chirps” that are supposedly “too quiet” to be heard?

### Section 33.1

Section 33.1 claims that the user interface of the Advantage provides for a higher level of undervotes or skipped contests by the voter. As mentioned earlier the available option to light all contests that the voter may vote should be enabled for an optimum user interface. Union County uses the worst possible configuration option, that of NOT lighting the contest names until they are fully voted. The report does not describe the academics’ findings regarding the Mercer County, New Jersey interface, which they state in Section 29.3 does have contest title lighting enabled. Perhaps they did not study this superior interface configuration?

### Section 34.3

The academics make a false statement in Section 34.3, claiming that “there is no indication” of which Party is activated once the voter is in the booth. To the contrary, there is an indication in the LCD that is also used to confirm voters’ selections. This indication consists of the party name corresponding to the activated ballot; and there would be a lit contest title if Union County would have enabled that option as previously described. In Section 34.4 the academics claim, without citing data or justification, that pollworkers and voters were confused by the alleged lack of party activation notification. The academics fail to mention that the pollworker display on the operator panel tells the pollworker what party is activated or if no party is activated.

### Section 35

Viewing the academics’ video regarding Section 35, the supposed ability to peer into the Advantage from the rear of the unit to determine how a voter is voting, shows that these assertions are false. While one can see the voter’s hand moving when it is close to the ballot face on the machine, it is not possible to see the voter’s finger actually pressing the selection button and thus determine how the voter voted.

### Section 36

Similarly, in their quest to improperly denigrate the Advantage, Section 36 holds the Advantage to the Federal 2002 standard, when it was certified to the 1990 standard that did not contain this requirement. The system complies with the standards to which it was certified.

### Section 38.5

In Section 38.5, the term "many" is subjective and needs to be appropriately defined by the academics.

### Section 39.3

In Section 39.3, the academics take the term Sequoia uses (cryptographic signature), assert its equivalence to a different term (digital signature), and then explain why what is implemented does not meet the requirements of the latter term. These sort of errors in the report lead to both faulty generalizations and faulty conclusions regarding Advantage architecture and security.

### Section 39.7

In Section 39.7, a hash of the vote data files, seeded with a machine-specific key, is computed and stored on each of the vote data files when polls are closed. It is beyond belief that the academics did not notice such, and hence the highlighted sentence and supposed conclusion of this section leads to questions regarding the rigor of their report and perhaps bias of the report writers.

In Section 39.7, footnote 82 is incorrect, and is contradicted by Section 39.8. Each ballot image, when stored, is protected with a CRC hash value.

### Section 40.7.1

In Section 40.7.1, the academics do not define a "true" cryptographic signature, unless the redefinition into "digital signature" in Section 39.3 is in force. The academics' definition in italics in this section is what is usually called a digital signature.

### Section 40.7.2

Section 40.7.2 is completely false. Please see the response to Section 39.7.

### Section 41.1

In Section 41.1, the "sometimes" that opens this assertion of the Advantage printing different results than are found on the Results Cartridge is not explained to be only in the extremely rare case of a machine failure during the few seconds where a voter's vote is being saved to the redundant memories. The academics' choice of "sometimes" is extremely misleading for an event that happened once across 10,000 Advantages and over 1 million votes cast.

### Section 42.2

In Section 42.2, the academics fail to mention that this CANNOT be done when the Advantage has an election loaded. The academics also fail to mention that even at the polling place once polls are closed that the pollworkers do not put the machines into the mode where the printing could be done. They also fail to mention that if such a reset were done, it would be immediately obvious, with no way to undo the situation. This is intellectually dishonest!

Sequoia challenges the academics to produce a video of the steps that must be taken and the responses and displays of the Advantage at each step!

### Section 45

Section 45 is irrelevant. Early Voting is not used in New Jersey as the academics should well know; it was implemented for one particular customer. This customer no longer uses the function (or the machines), but to avoid introducing bugs, the functionality was not removed in this version.

### Section 46

Section 46 is irrelevant. As the academics should know, consolidation of multiple voting machine results at the polling place is not used in New Jersey. However, the conclusions drawn in this section are erroneous anyway. In Section 46.3, the data from each Advantage is APPENDED to data already on the consolidation cartridge. Nothing is ever ADDED to totals already on the consolidation cartridge in the sense implied here where  $(-4) + (4)$  adds to zero. The conclusions reached in this section are erroneous. In Section 46.4, Footnote 90, the academics claims that the serial number could be suppressed on the report. Since the serial number is stored as binary, not text (ASCII characters), this is impossible.

### Section 47.11

Section 47.11 is an assertion without proof. In particular, there is no narrative on how such a modified cartridge would ensure that the internal memory would be kept identical to the manipulated cartridge. There is no detailing here at all.

### Section 48.6

In Section 48.6, the assertion about the ballot definition data is false. Depending on the details, there may not be any information about the parties, there may be minor spelling changes (i.e. "Democrat" vs. "Democratic" or "State Senate Dist 14" vs. "State Sen District 14", etc, etc) or other factors that obviate this simplistic idea.

### Section 51.5

In Section 51.5, the footnote "presumes" that code that was modified in 2001 was to meet the 2002 Voting System Standard that did not exist at the time the code was modified and introduced.

### Section 51.6

In Section 51.6, the academics omit the fact that the Advantage 9.00H firmware has been certified only to the 1990 FEC standards, not to the 2002 VSS. It is in the 2002 VSS that this specific coding practice was banned.

### Section 51.7

In reference to statements made by the academics in Section 51.7 and Footnote 97, unlike today's world of PC software with weekly updates and patches, Sequoia deliberately chose to stay with the solid, simple Lattice C compiler that existed when the Advantage was designed in the 1980s. In Footnote 98 of Section 51.7, the *fsize* example is false. Only one version of *fsize* exists for the Z80 firmware, which is in the main portion of the Advantage. Since the audio subsystem is separate, and compiled with different tools, of course it has a separate version of *fsize*.

### Section 52.5

In the last bullet item of Section 52.5, the academics again use the wrong version of the voting systems standards.

### Section 52.11

Section 52.11 is conjecture about a version that the academics were not even supposed to be reporting on and which is significantly different from the subject version of the Advantage.

### Section 54.7

In Section 54.7, the second bullet is incorrect. There is no library from Greenleaf Software used for the Z80 firmware.

### Section 54.13

In Section 54.13, can the academics point to any computing product that meets this requirement? This is an inflammatory statement. "Steal" is NOT a scientific or appropriate word to use in this section of the academics' report, let alone in the report itself. However, the term "steal" or its derivatives is used 115 times throughout what is purported to be a technical report. The entire premise behind Section 54 is inaccurate. The academics may not be aware that at least one of the third party vendors requested an opportunity to review copies of the Court documents requesting their product prior to turning it over to the academics. As with many software products, these products have licensing Agreements that bar customers, such as Sequoia, from turning over the vendor's property without providing notice to that product vendor.

### Section 57

In Section 57, the academics claim that when there is a failure, the Advantage gives no indication if the voter's vote is saved. This is false. The Advantage does indeed indicate an error when the vote data is not completely saved, with an indication of the step on which it failed. This is also written to the operator log. From the machine's error message, it is indeed possible to determine exactly what data was saved. In Section

57.19 and footnote 116, the source code examination must have been extremely superficial; there is no other explanation for the academics not noticing the variable *Syserr31* and how it is used (for example in *election\votesave.c* and *etool4\erhdlsup.c*). Section 57.21 is likewise false. Section 57.22 has no place here, though it does demonstrate the academics' personal biases toward paper based forms of voting. Additionally their statement is incorrect. Marginal marks, hesitation marks, and other forms of improperly made marks by the voter can cause the voter's intent to go unscanned by an optical scanner, leaving open the question posed by the report "did the machine record a vote?" even if that ballot is deposited in the ballot box.

In Section 61.1, the academics make an unfounded assumption that the structure of the Advantage D-10, the version of the product currently in the New Jersey State Certification process, environment is identical to that of 9.00H. It is not.

#### Section 62.5

In Section 62.5, the academics fail to note three things that make their sensational claim moot.

First, not one Advantage has ever been manufactured with the Program RAM chip installed.

Second, a very specific function must be invoked to cause this download; this is not available except before a ballot definition is loaded.

Third, as the academics do note elsewhere in their report, the downloaded code is in a RAM chip that is not battery backed-up, hence it will be cleared when powering off the machine.

Further, this version 8 is only 50 Advantages that are used in Mercer County. All other machines in NJ equaling 10,367 are Advantage 9s. Mercer County has decided on its own not to upgrade. These 50 units are used only as back-up and training machines.

#### Section 66, 67

Sections 66 & 67 are completely off-topic for this report. However, they do reinforce the presence of the academics' apparent biases in favor of paper-based voting solutions. The academics also ignore the visually impaired accessibility and usability challenges inherent in optical scan voting equipment.

## **THE APPENDICES TO THE ACADEMICS' REPORT**

### Appendix E

Related to Section E.16, E.22.1 and E22.4, the FEC standard that the 9.00H Advantage was certified to contains no such prohibition and related to Section E.17, the FEC standard that the 9.00H Advantage was certified to contain no such requirement.

#### Appendix H

Sections H.6 and H.7 imply that by cutting one of the 8 data lines connected to the printer, that only numbers would be misprinted. That is not the case – half of the alphabet would also be misprinted, making any such error extremely obvious. This is an example of more intellectual dishonesty. We challenge the academics to cut one of the wires so that only numbers are affected, no other characters.

#### Appendix J

With regard to the “fleeing voter” scenario in Section J using the Advantage, the comments in this section must be contrasted with a “fleeing voter” scenario in an optical scan environment, and any other voting technology. The same issues would occur across all voting technologies, and in all instances this scenario is handled procedurally by pollworkers in accordance with State laws.