

Preliminary Report to the Central Committee  
on the  
Riverside County Logic and Accuracy Testing  
Board.

Jeremiah Akin

I was appointed to represent the Peace and Freedom Party on the Logic and Accuracy Testing Board that met on 9 September 2003. The Riverside County Chair asked me to serve because I am a professional programmer familiar with many types of systems, and he hoped for an objective assessment from a qualified person of the functioning, reliability and security of the voting system used in Riverside County. He asked me to prepare a written report for the Central Committee before the 7 October election, and this is a preliminary report pending answers to a number of questions from the Riverside Registrar of Voters, who has stated that she will be unable to answer the questions until after the 7 October election.

**Brief summary.**

No one else on the Testing Board appeared to be technically qualified to understand the operation of the hardware or software involved in the casting and counting of votes in Riverside County. The test took longer than predicted, portions were performed outside the view of the Board, and everyone who signed the form stating that they had witnessed the test actually signed the form well before the test was complete. Statements made by the Registrar of Voters indicated to me that she is not qualified to assess the reliability and security of such systems, and that she misunderstands some essentials of computer programming and operation. Her deputies refused to answer some important questions. Some statements made by officials at the Registrar's office, and found on the contractor's website, I learned on the test day were misleading or inaccurate. Further research after the test day has turned up several other reasons to doubt the reliability, security and accuracy of the system. I strongly recommend that the Central Committee work with the Central Committees of other parties to insist on proper assessment and testing of the system, by technically qualified people who are given answers to all their questions and monitor the entire process.

**Section one – Events of 9 September 2003.**

The test was performed for the "Riverside County Logic and Accuracy Testing Board" meeting on September 9<sup>th</sup>, 2003. The meeting was held at the offices of the Riverside

County Registrar of Voters, and began a little after 10:00am. There were six observers present – one from the Libertarian Party, two from the Riverside County Grand Jury, one from the Women’s League of Voters, and one from the Republican Party (the Republican party member arrived late). I was there at the request of the Peace and Freedom Party.

The members of the observation group were greeted by Mischelle Townsend, Riverside County’s Registrar of Voters. She was in charge of the meeting, but was helped out by Brian Foss (Department Information Systems Coordinator), and later on by John Wilber.

Ms. Townsend began by saying that it was “terrible” that people questioned electronic voting. She said that the critics did not understand the whole election system and that they caused people to lose faith, without good reason, in the election process. (See Appendix 7)

Packets of information were handed out, containing news articles and a press release by Sequoia Voting Systems. Sequoia Voting Systems is the manufacturer of the electronic voting system that Riverside County purchased.

We were then given a review of sample ballots, absentee voting, polling sites, and so on—all topics listed on the Logic and Accuracy Testing Board agenda

But first, Ms. Townsend, who does not herself appear to have any real-world experience of computer programming, gave us a recap of her previous statements about people who question electronic voting systems. (See Appendix 4) She repeated that the computer scientists who question such systems are ignorant, and that the Sequoia system does not use Microsoft, which makes it more secure than those of companies that do use Microsoft.

She also stated that Sequoia’s operating system was “proprietary,” that is, owned by them, and secret; and this made it more secure than those products using Microsoft. Because it was secret, she said, no one could guess the commands needed to use it; therefore it was safer. (See Appendix 2 and Appendix 5 for details).

Mr. Foss and Ms. Townsend informed us that voting systems that did run on windows, such as Diebold, were not secure. They passed out a press release from Sequoia that said that the Microsoft system is well known and understood by hackers. (The article can be found at: <http://www.sequoiavote.com/article.php?id=50> )

(Later, I was to discover that these claims were disingenuous. Sequoia does, in fact, use Microsoft in key parts of their system. See Appendix 1 for details)

Ms. Townsend declared that Sequoia generates a “paper trail”. This is very important, since the critics of electronic voting have cited this as a minimum requirement for any trustworthy computer based voting system.

For example, if, after casting your votes on a touch-screen display, a printout of your ballot were to be generated behind a glass window, and, once you examined it and approved, it would drop into a locked ballot box; then--if there were any computer crashes, questions of fraud, etc.--the paper ballots could be counted by hand. Routine checks of randomly selected ballot boxes, could also confirm the system was working properly.

But this was not what Ms. Townsend described. Sequoia's "paper trail" is simply that, at the end of the day—with no voter verification—all information stored in each machine is printed out.

When asked, Ms. Townsend insisted that it would not be possible to create a true, voter-verified, paper trail, because printers are not reliable. The woman who represented the Libertarian Party objected, saying she gets printed receipts from stores all the time, and rarely sees any problems.

Ms. Townsend then countered that there was no reason to make a paper receipt because it would not serve any purpose that the electronic vote didn't already serve. She stated that this would be useless duplication of effort. (See Appendix 3)

It was now time for the official test of the system, the test that I, and other representatives of Riverside's political parties and other organizations, were here to witness.

### **The Test**

We were first taken to a room where we were shown the DRE (Direct Recording Equipment) card, a gray object, a little longer than a credit card, and several times as thick. It looked like a PCMCIA card that had been slightly modified. It is on this object that all the votes from each kiosk (voting terminal) are stored.

Mr. Foss told us several things about the card: that once it was inserted into the kiosk it could not be removed and plugged back into another one; if this occurred then the kiosk would shut down. We were also told that each card was individually marked for a specific kiosk and that a kiosk would not accept a different card.

After the polls closed, the data cards would then be removed and placed in a secure bag for transportation to a center where a tallying machine would record the votes of all kiosks in the County.

Our small group was then taken to a hallway where several voting kiosks were set up for the Logic and Accuracy test. We watched as the data cards that recorded the votes were loaded into the machines, and the test scripts were started. We did not verify the information that was loaded onto the test script cards. At that point we were told that the test process would take a while.

We were then taken to see a demonstration of a different type of system—not for electronic voting, but a machine for reading and counting the paper ballot cards submitted by absentee voters. The system, which was called DFM, optically reads ballots that have been marked by a Number 2 pencil. Some paper ballots were loaded into the machine, the machine ran, and then the results were printed out. It was a very short demonstration but no one saw any problem with it. Ms. Townsend, however, seemed to disparage this method, informing us that it was not as reliable as Electronic Voting.

Next, we were taken to the storage room where the voting machines were kept. The group was shown how each set of voting kiosks was stored and how they were labeled for pick-up and delivery.

We then went back to see how the test scripts on the electronic voting systems had progressed. It turned out that only a small portion of the test had been run and we were told that it would take several more hours to finish running the tests. If we came back after lunch, Mr. Foss said, we could watch the test results being collected and printed out.

Two of the people told Ms. Townsend they would not be able to return, and they'd like the results mailed to them. They then both signed some kind of document, and left.

I asked when the tests would be completed, and Mr. Foss said around 2:00 or 3:00 pm. I then returned home for lunch.

At 2:30, I returned to the County office, and asked for Mr. Foss. He came out, and took me into the back area, to the machines that had been running the tests. I was surprised to see that the test cards had already been removed. Mr. Foss asked someone who was wearing a Sequoia polo shirt what happened to the cards, and he was told they had already been pulled from the machines.

I was then shown a DRE card, and saw it inserted into the tallying machine—but I had no way of knowing if this was the same card that we had seen placed in the kiosk for the test. The results were printed out, and these supposedly confirmed the functioning of the system.

But since neither I, nor any of the other outside witnesses (as Mr. Foss confirmed to me) saw the data cards removed from the kiosks, it is not clear *what* was confirmed, if anything. It is possible that the cards I was told were those taken from the voting kiosks were switched, either intentionally or accidentally, with other cards before the results were pulled off of them.

In answer to a number of technical questions, Mr. Foss informed me that the results from the machine were actually stored in a database (Mr. Foss said a SQL Server database), and tallied on a Microsoft Windows machine.

I was very surprised at this discovery. I asked Mr. Foss how he and Ms. Townsend could have told us, so many times during the day, that the Sequoia system did not use Microsoft. Sequoia's proprietary software only covers a part of the system; the counting of votes is certainly no less important! He ignored the question, and did not look me in the eye. I asked Mr. Foss several times why no one mentioned that the voting tallying system ran on Microsoft Windows and each time he ignored my questions and would not make eye contact with me.

At this point, I must address one other significant matter. It was explained to us that the vote counting software can run in three modes: the pre-election testing mode, the election mode, and the post-election verification mode. Only one of these modes was shown to us – the pre-election testing mode. We were never shown how the software operates in the election mode. This means that the software was not tested in the configuration in which it would be used on election day. *The test did not cover what happens when the system is put in the election day mode or what happens when the system is put in the post election mode that is used to verify the results of the election mode.*

Also, the so-called “paper trail” aspect of the software was not tested. No paper record was created during the test. Sequoia says that one of the security measures that they perform is a manual recount of a percentage of the votes. This was also not done.

After I witnessed the failure to properly complete the test, I was asked to sign a form saying that I had witnessed the test being run and verified the results. I was dismayed to see that five people had signed the document already—even though no one else had returned to see the final results! (As confirmed by both Brian Foss and John Wilber.)

The text of the form reads: “We the undersigned declare that we observed the process of logic and accuracy testing of voting equipment performed by the Riverside County Registrar of Voters, as required by law and that all tests performed resulted in accurate voting of all units tested, including both touchscreen and absentee systems.”

I asked Mr. Foss why these people were allowed to sign when they hadn't seen the test results, but he just shrugged his shoulders and did not answer my question. I noted that the form had no place to indicate that the test was *not* completed successfully; so the document could give the misleading impression that the witnesses were unanimous.

I, of course, for the above stated reasons, could not in good conscience, sign the form; which caused the formerly friendly Brian Foss to become visibly angry. I carefully enumerated the reasons why I felt the test had not been properly completed, but Mr. Foss kept demanding to know why I thought the test wasn't successful—and then refused to counter, or even listen to, the points I raised.

He was belittling in the way he asked me why I didn't agree with the statement on the form. At one point he even hissed at me because I wasn't going to sign the form. I told him not to hiss at me, and he replied by saying “I'll hiss at anyone I want!”

Needless to say, this is not appropriate behavior. It is not okay to insult someone who is there to verify that a test was completed successfully just because he did not agree that the test had been run correctly. I felt that this insult was an attempt to try to embarrass me into signing the paper.

I asked for a copy of the form but was told by John Wilber that I could not get one unless I agreed to sign it. (A copy was later provided to the Peace and Freedom Party County Chair when he requested it from Michelle Townsend.)

At about 3:50 I left the county building, needing to get back to work writing software for my clients.

## **Section 2 – analysis of what happened**

On the Sequoia web site it says: “The key to election security is in the people and policies that govern the use of voting equipment as much as it is in the design of each voting system.”

It is unfortunate that Sequoia and Registrar of Voters for Riverside County did not live up to this statement. The form used to verify that the test was completed and verified is invalid. It was signed by people who did not witness the test being completed. This begs the question, how many other tests were signed off before they were completed? How many other forms have invalid signatures on them? A person can read Sequoia’s website and listen to Michelle Townsend tell you that there are multiple checks in the system. But if the Sequoia software company and the Riverside County registrar of voters were not willing or able to make sure that this test was run correctly, how do we know that any of the other tests were run correctly? How do we know that some other check that is more important has been done correctly? How do we know that other forms were not signed before tests finished?

My four main complaints are:

- 1) The voting test was not done correctly. The data storage cards that kept the votes on them were not removed in front of the people who were there to verify the testing of the electronic voting system. Without someone to watch the cards as they were removed from the kiosks and put into the card reader, it is not known that the results that were printed out by the system were the results that were on the card. It is a shame that this very important step was done with no one around to witness it. These conditions allowed the opportunity for someone to pull the data holding cards and then replace them with different cards in the reader.

In addition to not having the test completely observed, the test did not completely cover the system. There were important portions of the vote counting software that were not tested. The vote counting software can run in three modes – the pre-election testing mode, the election mode, and the post-election verification mode. Only one of these modes was shown to me – the pre-election testing mode. The election day mode and post-election verification mode were not tested.

Also, the paper trail aspect of the software was not tested. No paper trail was created during the test. Michelle Townsend and Brian Foss both said that one of the security measures that is performed is a manual recount of a percentage of the votes. This was also not done during the test. The test, in addition to not being completely performed in front of the monitoring group, did not accurately reproduce what Sequoia and Riverside County say will happen on the day of the election.

2) A document meant to verify that the test was completed and that the results were verified was not filled out correctly. The first five people who signed the form signed it before the test was completed. The form is not valid because people signed that they witnessed something that they could not possibly have witnessed. I did not believe that the test had been run properly, so I did not sign the form. I believe that both Brian Foss and John Wilber tried to pressure me into signing the form and that Brian Foss treated me poorly because I would not agree to sign it.

The form did not have a place to indicate that a person did not agree the test had been completed. This means that as long as a few of the people signed the form it could give the appearance that there was total agreement on the test. A portion of the form needs to be set aside so that people who did not agree with the statement could also have their opinion recorded. By design, the form excludes all dissenting opinions.

3) I, along with the other people at the meeting, were given *seriously inaccurate* statements about the structure of the Sequoia voting system by both Michelle Townsend and Brian Foss. These inaccurate and misleading statements have also been published by Sequoia on their website and were handed out, by Michelle Townsend, in a packet of information that was given to everyone at the testing board. I along with the other people at the testing board were told numerous times, by both Mrs. Townsend and Mr. Foss, that the Sequoia voting system does not rely on the Microsoft Operating System and is more secure because it uses a proprietary software system. While it is true that some parts of the Sequoia voting system do run on a proprietary operating system, there are critical parts of the system that do in fact run on the Microsoft operating system. By the time that the part of the system that runs on Microsoft was exposed, most people had left, having been told that it was OK to leave before the test was finished because the results would be mailed to them.

4) While Mrs. Townsend and Mr. Foss talked a lot about making the system secure, they did not mention any process that would make the system bug free. They said that the code was reviewed by a third party, but that is only the code that Sequoia wrote and does not cover other programs that get used during the vote tallying, and reporting phase of the

election process. Since they use Microsoft windows they would have to be able to guarantee that there was no bug in that operating system to guarantee that no bug could affect the vote tallying process. The same goes for the database they use, the drivers they use for the card reading hardware, the printer drivers, and any other third-party components that they use in the system. Do we really want to have people doubt the outcome of the election because we do not know if a bug did affect the vote counting and reporting processes?

Not enough attention was paid to how many bugs are in the voting system and the possible effects of bugs on the election process. Mischelle Townsend said that the code review by Wylie Labs covered both bugs and security problems. She assured the group that the program was searched through in a line by line, preventing these from occurring. (Anyone with even a little bit of experience with writing software knows that you can not eliminate every single bug in complex software – even if you perform extensive tests and code reviews.)

The main threat to an election result from computer systems does not come from security, but from software bugs. There is no method for developing complex software that is bug free. This is presumably why Sequoia fails to mention software bugs on their web site. Sequoia simply can not claim that they know they have no bugs in their software. Do we really want people to doubt the outcome of an election because the software that was used to capture and count the votes had software bugs in it?

Strangely, I can not even find any mention of software bugs on Sequoia's web site. Since a software bug could cause all kinds of problems in the system, from a vote being counted wrong, to a vote being lost, you would think that they would want to address this issue.

It is very important that this test gets performed again with people from the public able to watch. The public deserves a chance to watch the software that counts their votes be tested properly and thoroughly. The public also deserves to know that the Registrar of Voters will not collect invalid signatures on a form that says the test passed, as according to law, and that the results were verified.

## Appendix 1

### Misleading claims about the voting system

Sequoia gives a very misleading image of their system. They say that they use a proprietary system that is more secure than Microsoft. On their web site they cite the fact that they don't use Microsoft in their voting kiosks as a reason why they are more secure than their competitors, like Diebold. (Diebold did a poor job of keeping their code secret. They placed it on a company ftp site that allowed anonymous access. An analysis of the code was done by John Hopkins University) Many of the problems found with the Diebold system were related to the fact that it uses Microsoft as the underlying operating system. Sequoia has released an article (<http://www.sequoiavote.com/article.php?id=50>) that states that they do not have the same kinds of security problems that Diebold has because they use a proprietary operating system. The aforementioned report states:

“Sequoia's Proprietary Operating System vs. Diebold's Use of Microsoft Windows

While Diebold relies on a Microsoft operating system that is well known and understood by computer hackers, Sequoia's AVC Edge runs on a proprietary operating system that is designed solely for the conduct of elections.”

This is a very misleading statement. The system that Sequoia has is composed of two sub systems, the voting collecting system, and the vote tallying system. The vote collecting part of the system is made up of one of the two models of touchscreen kiosks that Sequoia sells. We are told that the kiosks use a proprietary system. The vote tallying system is called WinEDS and it runs on the Microsoft operating system.

On their web site, Sequoia does not explicitly disclose the fact that they use at least one Microsoft product, which I find to be misleading. If you carefully examine the above statement it says “Sequoia's AVC Edge runs on a proprietary operating system that is designed solely for the conduct of elections” which is technically true but *not the whole truth*. Of course they would not want to mention that the software that actually counts the votes runs on the Microsoft platform in the same article where they admit that the Microsoft operating system “... is well known and understood by computer hackers...” If Sequoia wants to be considered an open, honest company they must be completely forthright about their system. They must tell people exactly what their system is made up of in a way that is not misleading. Doing anything less than that will only make people not trust the company's system, and therefore, not trust the outcome of elections that are decided by it.

I could only find one description of the Microsoft Windows based vote tallying software on Sequoia's web site( The same description was repeated in 2 places on the site). This is the description :

“WinEDS, the ‘Elections Database System for Windows’ is Sequoia’s client-server based computer network system. WinEDS is used to administer all phases of the election cycle, create electronic ballots for the AVC Edge, and tally early voting, as well as official election and absentee votes. WinEDS provides a flexible, easy to use reporting and information processing tool for the election administrator.” (link: <http://www.sequoiavote.com/docs/AVCEdge.pdf>)

This statement does not make it explicitly clear that they use Microsoft Windows instead of some other windowing system, such as X Windows, or some proprietary windowing system. I could not find anywhere on their site where they specifically said that they run software on the Microsoft Operating System. The few times that the Sequoia web site mentioned the WinEDS program should be compared to the numerous times they said they used a proprietary system that was “impossible to hack.”

Sequoia states that they use the WinEDS program to administer “all phases of the election cycle”, meaning that if there is a bug or a security flaw in either WinEDS, or any of the third party components that it may use, all phases of the election cycle may be influenced by it. Sequoia states that the software is used for reporting. This is the same software that reads the ballots captured in the data cards. So if there is an error in capturing the data, it could trickle down into the reporting functions of the WinEDS application. If the data is read wrong and then printed out wrong by the same program, you could have the “paper trail” and all the other audits that Sequoia claims to have, match the data that was collected incorrectly. If this program is being used to tally the votes and print out the “paper trail” we need to be sure that it is both bug free and does not have any security flaws in it. Microsoft Windows, which this program runs on, has many security flaws and bugs, making it an exceedingly poor choice from both a security and software bug stand point. The question of why Sequoia chose to use a platform that they say “... is well known and understood by computer hackers...” needs to be answered.

If the software that reads and counts the votes has problems with bugs or security it does not matter how secure or bug free the system that collects the votes is. All the votes can be collected correctly – but if there is security problem or software bug in the underlying system of the tallying software, then we can not know that the count was made or reported correctly.

Sequoia needs to come clean about any 3<sup>rd</sup>-party software, such as databases, that they use in any of their products. The security certification level of every product that Sequoia uses should be disclosed to the public.

## Appendix 2

### Security Through Obscurity

Mischelle Townsend says that the Sequoia operating system is more secure because it is proprietary and people do not know what commands to use to hack into it. This method of attempting to keep a system secure is known as “Security through Obscurity”. There are two major flaws in using this type of security. First, it offers no protection from insiders. Even if the system is successfully guarded from the general public, someone on the inside who has knowledge of the system can manipulate it. Secondly, this type of “security” requires that the system never falls into anyone else’s hands. This is far more difficult than people might think. Diebold systems, a competitor to Sequoia who also attempted to use Security through Obscurity, failed miserably in keeping their code out of other people’s hands.

A member of the public trusting Security through Obscurity with voter systems would be like a person trusting a casino that says, “I’ll deal you your cards under the table so no one else can see them.” This might guarantee that no other customer at the table sees your cards, but how do you know that the casino is dealing the cards properly? The public may be told that there are too many checks for any type of tampering to happen, but we are not told exactly what every security precaution is. It is easy to say that you have a check to prevent something if you never are required to show proof that the check exists. Would you believe a casino who says they have security measures to make sure that cards dealt to you under the table are dealt fairly, but they won’t tell you what those security measures are? Would you be willing to bet your money at a casino that uses this type of “security”?

People who use or trust Security through Obscurity often do not realize how hard it is to insure that a system remains obscure. The fact that it is incredibly hard to keep a system secret is one of the reasons why there are so many proprietary programs out there that have security flaws in them. To insure that your code does not slip into someone else’s hands you must have an extreme level of security not only around every copy of the code, but also around any documentation of the system and around all the people who work with the code. What happens if the source code for the Sequoia gets sold to someone by a disgruntled employee? Ms. Townsend said that there are too many checks in the system to allow this to happen, but she would not explain what they are. Can we be sure that there is adequate physical security around the building where Sequoia keeps its source code? Is this level of security the same around all places where the source code is kept? Do we know that each employee is searched before they leave the building to make sure that they are not taking the source code home so they can sell it to the highest bidder? Do we know that an employee has not smuggled the compiler for Sequoia’s system out and sold it to someone? Billions of dollars can be lost or won by companies depending on elections. The path of our foreign policy can be decided by who wins an election. Could some company or some other international interest threaten someone, or threaten their family, causing them to reveal their knowledge about the system? Or possibly steal a

manual or source code from Sequoia? Do the custodial staff and night watch people, if they exist, get searched? If the search exists is it tough enough? Even if every one is searched completely, what would stop someone from simply telling what they know about the code or the network set up, etc?

There are many proprietary programs that are not secure. For example, the Microsoft Operating System is proprietary, but people still are able to hack into it. The Diebold software was proprietary but people managed to get hold of the code and figure out how it worked.

The method of hiding source code from everyone who did not develop it does not offer any protection from the people who develop the software. Even if no one outside Sequoia could figure out how to penetrate the system, we would still have to worry about people inside the company planting malicious code in the software. An inside job could be much harder to detect than an outside job. For example, a code that has been carefully reviewed for security flaws could be compiled by a modified compiler that inserts a security flaw. This kind of security flaw could be undetected in code reviews but could be executed by someone inside the company. If Sequoia is going try to make their software secure from outside hackers by hiding the source, they need to explain how they are keeping it secure from inside hackers. We need to know what kind of security measures are taken to prevent this.

The public needs a transparent system so they can see what security checks are actually in place and decide if they make the system secure enough for them to trust. If the public has the checks hidden from them, then we can not make an informed decision about how secure the system really is.

## Appendix 3

### Loose Definition of the Phrase “Paper Trail”

Sequoia Voting systems claims to be able to make a paper trail that will verify the correctness of the electronic voting system, but the process for making the paper trail is opaque. Handing out a printout that matches what a computer system displays on a screen is not a paper trail. No matter how many checks you put in the voting kiosks to make sure that something doesn't get modified, if you use a bug infested and un-secure operating system to count votes and produce a “paper trail” of that vote, it is legitimate to be skeptical of the results.

Furthermore – we were not shown where the print out of the votes occurs. If the printout comes from the windows based system that they use for tallying votes, or some other windows based system, then the validity of the printouts can be legitimately questioned. Do the printouts come from printers that are networked to other machines? Could a printer be modified in advance to receive information from another computer (either on a wired or wireless network) so that it printed out false results? Are the printers that print out the “paper trail” inspected and sealed before they are used? If not then it remains a possibility that they are compromised and can print out false results.

Mrs. Townsend said that there would be no reason to make a voter verified printout of each vote. This strikes me as absolutely wrong. A voter verified paper trail is something external to the computer system that the computer system can be checked against. If you have a “paper trail” that is not voter verified then you lose the ability to check your computer against an outside source.

In the 2002 election in Florida, Palm Beach County used Sequoia's touchscreen voting system. The touchscreen system did not record 78 ballots. Sequoia insists that 78 people came to the polls and decided not to vote. To many people, myself included, this sounds suspicious. It seems much more likely that some bug in the software caused those results. I have met a lot of people who do not vote, but I haven't met a non-voter who goes to the polls, signs in, and then doesn't cast a vote. If you aren't going to vote it's easier to just not go to the polls. Since we are not allowed to investigate the source code that the computer was using, and we do not have a voter verified paper trail, we can really never know what happened there.

Even if each electronic ballot is kept securely, what is to stop someone from hacking into the vote tallying software that produces the elections results and prints out the reports? After all, the program that Sequoia loads the data cards onto runs on an operating system that is described by Sequoia themselves as “well known and understood by computer hackers”.

For a real paper trail it is necessary to have a print out of the vote, have a person verify that the printout matches what they voted for, and then have the printout stored in a secure location where it cannot be modified. If there is no voter verification of the printout, it is possible that the voting software would display one thing on the screen and then, without the person knowing it, print out something else.

There are many times when I have gone into a grocery store and purchased something that was marked at one price and rung up at another price. In fact, this is a common occurrence at many stores. Certain supermarket chains have been cited in California and elsewhere. And anyone who checks receipts, especially on sales items, will discover how common this is.

Fortunately, stores give out paper receipts at the end of every transaction that list what has happened. This allows a person to check to make sure that the computer system that was used to ring up the purchased products did this in a correct manner.

What would happen if this situation was a little bit different? What if the stores, instead of giving you a receipt of the transaction, just told you what the total amount due was? If you asked to see your receipt, the cashier would say, don't worry we print them all out at the end of the day to make sure that no one was incorrectly charged. If you asked to see your receipt at the end of the day you would be told that it is not possible. If you insisted that what was really happening was that you were getting no receipt at all the store would reply by saying that you do get a receipt, you just aren't allowed to see it. The store would also assure you that they know that all the transactions were rung up correctly because the number of receipts printed out matches the number of purchases made and that the receipts match our computer records of the transactions 100% of the time, so there is no way that you could be cheated without someone knowing about it?

How long would you continue to shop at that store?

Passing off what gets printed out at the end of an election day as a "paper trail" instead of just a paper report of what is in the Sequoia system, makes about as much sense as saying that receipts from stores that never get verified by the customer would protect the customer from being overcharged.

Sequoia has some very interesting complaints about making a printer trail. For example they complain that it would be hard to make sure that the printers didn't jam up and that it would be hard to make sure there was enough paper at every polling place. (Last time I checked our country was capable of landing men on the moon. Does Sequoia really think that problems like getting enough paper to a polling station are insurmountable for the American people? ) The most interesting complaint I have heard from Sequoia ([http://www.lasvegasweekly.com/2003/05\\_08/news\\_coverstory.html](http://www.lasvegasweekly.com/2003/05_08/news_coverstory.html)) is that people who look at the paper trial that is printed out would say "That's not how I voted." – How could it possibly be bad for someone to point out that the system didn't record what they voted for? This is exactly why paper receipts are needed – so that people can verify that the

system recorded the vote that they wanted. It appears that Sequoia thinks that it would be a bad thing for someone to notice that the system didn't record their vote correctly.

## Appendix 4

### Straw Man Arguments and Pseudo-Reason

Mrs. Townsend should be called on her straw-man arguments about the positions of computer scientists who oppose closed source voting systems. Mrs. Townsend insisted that the computer scientists complain that there is no paper trail in Sequoia's electronic voting systems, when in fact, according to her, there is. This is a great example of what a straw man argument is. What computer scientists worry about is that there is no voter-verified paper trail (Dr. Dill's petition). Mrs. Townsend carefully leaves the words "voter verified" out of her argument to make it seem like computer scientists insist that there is no paper trail like the type of "paper trail" that Sequoia makes. By not properly explaining what the computer scientists' position is, it makes it easier to "win" the argument with them about paper trails. She attempts to make computer scientists look like fools for complaining that something doesn't exist when it does. The problem is that computer scientists are making a different claim than the one she is refuting. This does not make the computer scientists look foolish, instead it just makes Mrs. Townsend look like she either doesn't understand the position or is intentionally misrepresenting it.

In addition, Mrs. Townsend does not fully address the concerns of the computer science community. The computer science community is just as worried about software bugs as they are about security. Even line by line code reviews can not catch every bug in a system as complex as the one that Sequoia has produced. This is an important fact. One of the main criticisms of the computer scientist community is never adequately addressed. Leaving out a major point of concern that the computer scientist brings up makes it easier for someone to "refute" the claims that they make.

Mrs. Townsend tries to say that because there is no proof that election fraud has happened in the past, that it must not be possible. In a Washington Post article Mrs. Townsend stated, "If the computer scientists had one valid point, one, then why hasn't one incident of what they're saying occurred in all of these elections?" (<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A42085-2003Aug10>). This is an astonishingly silly argument. Am I supposed to believe that since no one has robbed a particular bank that it is impossible for someone to rob that bank in the future? Because we can't prove that it happened in the past it must not be possible? We also need to keep something in mind about this statement. Fraud with this type of system has not been proven. That does not mean that it has not happened. Since the companies that control the code that counts the votes will not let us examine it, we can not know if election fraud has been committed with it. The companies withhold key pieces of evidence that could show that election fraud did or did not happen, and then say that there is no proof that it has happened.

Mrs. Townsend also acts as if she has more knowledge of computer systems and computer security than she has. She has no real world experience with programming or computer security. This should be duly noted when she gives her opinions about people

who have PhDs in computer science and teach in prestigious universities. For example, Dr. Rebecca Mercuri did her PhD on *Electronic Vote Tabulation: Checks and Balances*. Mischelle Townsend would like you to think that everyone who doesn't agree with her is ignorant, or has a chip on their shoulder, or is in some other way unqualified to even question the electronic voting system that she advocates. The truth is that a significantly large group that is comprised of people who have PhDs from, or teach at, places like Stanford, MIT, Harvard, etc – some of the brightest minds our nation has produced – have serious reservations about the type of system that Sequoia has sold to Riverside County.

## Appendix 5

### Sequoia's Use of SHA-1

I find it very interesting that while Sequoia claims that opening their code up to public review would hurt security, they use a cryptology standard that is open for public review.

In Sequoia's press release titled "Sequoia Discusses Safeguards of Electronic Voting...July 30, 2003" found here: <http://www.sequoiavote.com/article.php?id=50>

Sequoia states: "Edge smart cards are encrypted using properly initialized DES and signed using SHA-1, as recommended by the Johns Hopkins researchers."

SHA-1 is a publicly known encryption method used for guaranteeing the integrity of a message or file. SHA-1 is developed by NIST (the National Institute of Standards and Technology), who encourages public review of their cryptology. NIST produces FIPS (Federal Information Processing Standards) for the public to review. Anyone can download the FIPS for SHA-1 from the NIST website (<http://www.itl.nist.gov/fipspubs/fip180-1.htm>). This means that anyone can find out the details of this encryption algorithm. If there was any problem with the SHA-1 standard then there would be two important consequences. 1) Any code that implements this standard would have the same flaw. 2) Any one could find out about this flaw.

If Sequoia is correct that being open for public review makes a system un-secure then they must admit that the encryption method that they use is un-secure. The simple fact is that it is possible to make something both secure and open to public review, as evidenced by the cryptology that is open for public review by NIST.

How can Sequoia insist that they need to keep their source closed to ensure security while that very source code uses security measures that are open for public review?

## Appendix 6

### Incomplete Code Escrow

Alfie Charles of Sequoia software says, “Security procedures also guard against tampering, Charles says. For example, immediately before an election Sequoia gives a copy of the voting software to state officials to lock up. That copy can later be checked against the software actually running on the machines if any question of the election's integrity is raised after the polls close.” (link to article: <http://www.securityfocus.com/news/2197>)

Before an election Sequoia submits its code to the Secretary of State's office. This process is called code escrow. If someone thinks the system has been tampered with then they can take the original code and compare it to the deployed code. This is supposed to verify that the system was not tampered with.

At first this sounds like a great check. Sequoia wants the public to think that if someone was somehow able to modify the code that runs the voting system there would be no chance that they could do it without being caught. If they modified the system, a check would be run and differences between the code bases would be evident. Unfortunately, This is not necessarily true. Why? Because Sequoia uses a Microsoft Windows application to count the votes. This means that the software for counting votes runs on top of the Microsoft Operating System. In turn, this means that code written by Microsoft needs to be executed in order for the program that tallies votes to be run. If a person modifies the components of the Microsoft system that the Sequoia software uses, then it is possible that they can modify the data that is either stored, analyzed, or printed out by the vote tallying software. These types of modifications can be done without change to the Sequoia code. Therefore an analysis of the code written by Sequoia would not guarantee that the software used to tally the votes was free of tampering. If Sequoia wants to make this type of code lock-up safety check work, they have to make sure that *all the code that gets executed, not just the code that they write*, gets locked up. The way that Sequoia implements code escrow reduces it to nothing more than a fancy PR stunt.

## Appendix 7

Don't question electron voting ... unless you are me!

Mrs. Townsend throughout the day insisted that it was a bad thing to question electronic voting systems. She went as far as saying that it was a terrible thing to do. She has also been quoted in the press as saying it is bad to question electronic voting system. I think that it is outrageous to say that a person should not question a system for counting votes that is not transparent. It should be noted that Mrs. Townsend herself said that the Diebold system was not secure. It seems weird for someone who says that questioning electronic voting security damages voter's confidence in the election system, to then question the security of an electric voting system that is deployed in more than half the states. Mrs. Townsend doesn't mind when people criticize voting systems that she did not select, but as soon as they criticize the voting system that she did select, they are doing a terrible thing.

## Appendix 8

### Questions Not Yet Answered

Some questions I asked were not answered on 9 September, and other questions occurred to me later as I researched the Sequoia system. On Monday 22 September the Riverside County Chair of the Peace and Freedom Party (my father, Kevin Akin) left a list of 25 questions for Mischelle Townsend at the Registrar's office, as she was not then available. She answered the first five, which all asked for the names and titles of her employees or members of the Logic and Accuracy Observation Board, in a letter dated 25 September. In this letter, she promised to provide answers to the remaining questions after the 7 October special election. Those answers are thus not available at the time of completion of this preliminary report. To give a better picture of the areas in which additional information will be helpful in the preparation of a final report, the not-yet-answered questions are given here.

6. Is the database kept on the same machine as the vote-tallying software, or is it kept on a different machine?
7. If on a different machine, where is it physically located?
8. Are you aware of other machines made by Sequoia that have failed to perform during elections?
9. Which failures are you aware of?
10. Are you aware that these machines were certified?
11. Who did the code review for the vote tallying software that runs on Microsoft Windows?
12. When was the last time that the software that is run during elections and vote-counting had a code review? Which software was reviewed when?
13. What other software is installed on the Windows machine that the vote tallying software is on?

14. When you told the observers that the voting software Riverside County uses does not run on Microsoft Windows, were you aware at that time that the vote counting software does in fact un on Microsoft Windows?

15. How often do security patches get applied to the computer that has the vote tallying software installed on it?

16. Is the computer that has the vote tallying software installed on it hooked up to the internet?

17. Can someone access the internet from that computer?

18. If it is hooked up to a network, how many other machines are on the network and how many people use them?

19. Is the software that tallies the votes (the windows program) the same program that produces the reports?

20. What is the name of the program that produces the reports?

21. What kind of debugging methods does Sequoia use?

22. What kind of security certification does the network at the Riverside County Registrar of Voters office have?

23. Are you aware that Sequoia uses the SHA-1 encryption standard?

24. Are you aware that the details of this encryption standard are open to public review (anyone in the public has access to the details of the encryption algorithm)?

25. During previous observed tests, have some people signed the paper stating that they have observed the tests and that the tests were satisfactory, although they in fact left before the tests were completed?