Maricopa County Elections:

A Security Report for the Maricopa
Libertarian, Republican and Democratic Parties

OVERVIEW AND EXECUTIVE BRIEFING

Attached find a 24 page document summarizing the state of election integrity and security issues in Maricopa County AZ during on and around the Feb. 5th 2008 Presidential Preference primary election.

The reports draws on several sources:

- Our detailed study of the Sequoia voting systems by way of internal Sequoia documentation, the California Secretary of State's 2007 "top to bottom" security review of voting systems and conversations with a former Sequoia employee.

- Our study of public records provided by Maricopa County under Arizona's FOIA-equivalent laws.

- Our on-site observations before, during and after the election[1].

- A review of the legalities surrounding the Federal voting system certification process and how it interacts with Arizona law affected **Appendix A**[2].

Assembling and viewing this material in total, a disturbing picture emerges of a department that is fighting transparency and observation at every level any by any means possible (legal or otherwise), a voting system vendor that is visibly cheating on their legal requirements (and security model) and a series of interlocking bureaucracies at the county, state and federal levels that together are supporting the unsupportable.

The report contains concrete examples of these problems and where possible suggests mitigations.

By showing the interweaving issues between the levels of government, it forms a work that is valuable to anyone in America interested in fair, honest and transparent elections. We have run into a situation in this one (large) county that forms a microcosm of what's wrong with America's democratic process.

This isn't the report we set out to write. At first we thought we would be producing something specific to the Maricopa or at least Arizona electoral situation. That core purpose is still present and still useful. But we urge any reader to look past the local, specific issues and pay attention to the broad strokes.

We're all in trouble. We write this as a plea for help, as an effort to expose something tragically wrong.

Thank you for your time and attention in reading what we've fought to produce.

*NOTE: **Appendix A** covering Sequoia's legal situation is of national interest and sheds light on flaws not just on Sequoia's product line, but the entire electronic voting infrastructure via the federally-approved testing labs and Sequoia's apparent subversion of that process.*

Jim March - 1.jim.march@gmail.com / *John Brakey* - auditaz@cox.net / *Michael Shelby* - mshelbyinaz@cox.net

---

1 We wish to thank Mr. Jim Iannuzo, Maricopa Libertarian party chair for issuing us party observer credentials and Mr. Michael Kielsky, AZ state Libertarian Party chair and attorney at law for calling an emergency court hearing to force the county to accept LP observer credentials. This report would have been impossible without their timely support.

2 Here we must acknowledge the research of Dr. Tom Ryan, former SAIC programmer.

Maricopa County Elections:

A Security Report for the Maricopa
Libertarian, Republican and Democratic Parties
Mar. 7th 2008

Jim March, John Brakey and Michael Shelby

Conceptual Introduction

It's well established that Arizona elections must be conducted under public and party observation. As you read this report, realize that in the electronic age, the nature of "observation" must change in order for the core intent of existing law to remain effective. That intent is that the counting of votes be a public, transparent process.

No new legislation is needed to ensure electronic observation and electronic transparency of electronic elections. All that's needed is an attitude shift. Without such a shift, without a commitment to a transparent process, elections will be stolen – the only questions are "when?" and "under whose watch?" When innocent glitches occur, doubt will abound.

The authors of this document are committed to election transparency, and herein hope to show why it's needed and where it's lacking.

Where possible, we will suggest process improvements.

We will try to show, where possible, how a transparency flaw in the electronic voting system would be viewed in an equivalent failure in the pre-electronic age – circa 1880 using 1880-period technology. This analogy won't always work, but where it does we think it can aid understanding of the "computer tech" issues for non-technical readers. (1880 post-dates private voting, pre-dates lever machines.)

Additional Scope And Notes

As we'll show in Section 1, there is an oddity in the numbers for the GOP vote; the way the county is reporting the mail-in vote totals adds to what we HOPE is confusion.

Sequoia Voting Systems manufactures the computerized election equipment used in Maricopa County. Recent revelations by a former Sequoia employee, corroborated by technical examination reports commissioned by the States of California and Pennsylvania, show that an entire subsection of the Sequoia product line known as the Ballot Preparation Software ("BPS") essential to program ballot definitions in elections, was withheld from mandatory certification review at the federal and state levels. This constitutes a fraud committed by Sequoia Voting Systems committed at the state and federal levels. We'll discuss Sequoia and BPS in more detail in Appendix A.

The main goal of this document is to reveal the current level of transparency and security in the Maricopa Elections Division today, with suggested improvements in most cases. Appendix B covers the confusion over the permanent early voting roster being experienced by too many voters.

1. Vote Totals And Patterns Based On Official Summary Sheets (Before Provisionals).

	Early Vote Totals	EVT%	Precinct Totals	PT%	Total Votes	TV%
McCain	115,764	51.37%	51,953	41.60%	167,717	47.89%
Romney	63,429	28.15%	53,566	42.89%	116,995	33.40%
Huckabee	18,533	8.22%	10,176	8.15%	28,709	8.20%
Paul	8,569	3.80%	6,537	5.23%	15,106	4.31%
Giuliani	10,364	4.60%	1,041	0.83%	11,405	3.26%
Thompson	6,789	3.01%	659	0.53%	7,448	2.13%
Hunter	632	0.28%	160	0.13%	792	0.23%
Keyes	369	0.16%	231	0.18%	600	0.17%
Other	902	0.40%	572	0.46%	1,474	0.42%

1a) When we run the same numbers for the Democratic side, we don't see any massive shift in vote pattern between the two front runners (Clinton, Obama) from the mail-in vote to the precinct vote. The shift we do see is easily explained by Edwards dropping out prior to election day.

On the GOP chart above we see a shift in voting patterns between the mail-in and precinct votes. It might be explainable as a sudden conservative shift away from McCain. More investigation is needed but meanwhile analyzing the numbers points to problems in the Maricopa reporting system:

1b) Next, we must note that once the mail-in vote totals were reported on election night, **they were never reported as increasing later.** That means that mail-in ballots sent to the voters and then dropped off at the polling places (which is legal) were recorded as precinct votes. But they're not treated the same. Early drop-off votes don't go into the precinct optical scanner, but rather a separate bin that is tabulated later at elections HQ as early votes. Other counties such as Pima process AND report their precinct drop-off mail-in votes as early voting instead of precinct voting.

There's a reason for this: it's necessary to figure out which votes are which in order to make sure voters don't vote twice: mail-in and precinct. Mis-reporting mail-in votes as precinct would have the effect of "smoothing" the numbers above to some degree. If the mail-in votes are favoring McCain to this level, tossing some mail-in votes into the precinct vote totals will have a leveling effect – in other words, if Maricopa County had reported mail-in vote totals properly, the difference in vote pattern between mail-in and precinct votes would have been even more extreme.

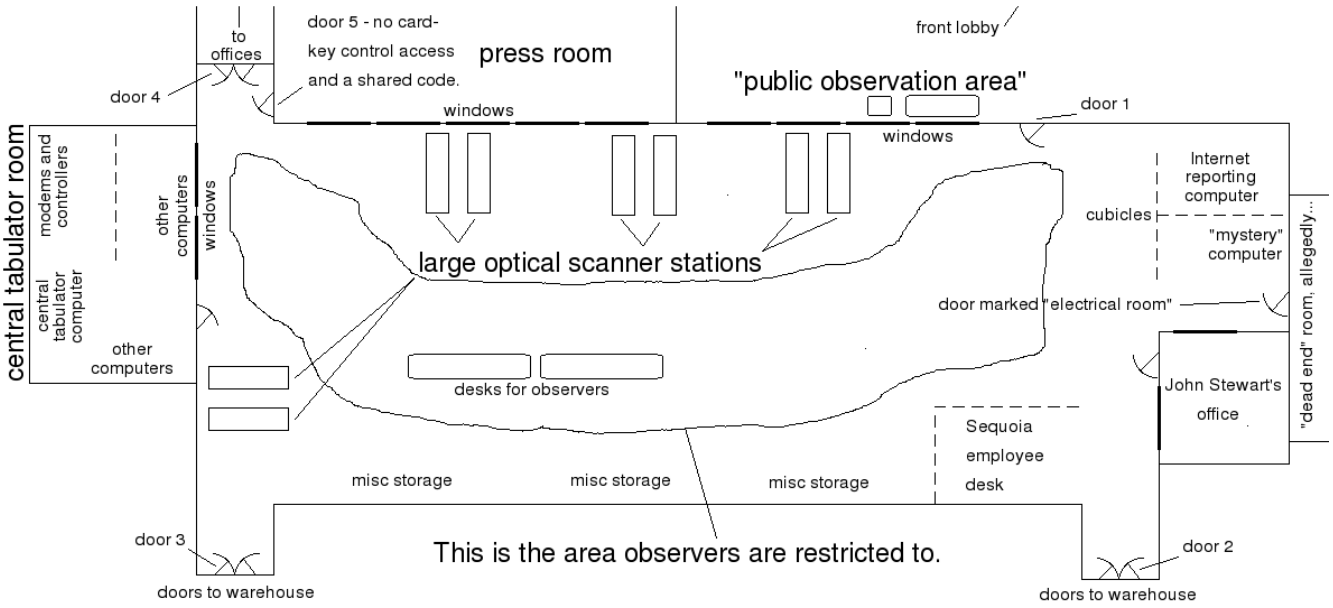
2. Precinct Access, Pollworker Staffing And Long Lines

There are 1,142 precincts in Maricopa County. According to Karen Osborne, by law, the elections office can only open 50% of the precincts in a party primary election of this sort. She opened 397 precincts, only 34.8%. Staffing per-precinct appeared minimal per our sources among pollworkers. This caused long lines, frustrated voters who took out their anger on the pollworkers and pollworkers with no breaks even for restroom access. We consider this unprofessional and abusive. Some pollworkers will never return. There were an average of 130 provisional votes per precinct, which is completely unprecedented. Something was wrong; we suspect this situation was engineered to advance the case for all-mail voting. Increasing voter wait times and line lengths to suppress working-class voters at the peak periods of election day is an old trick. What happened here may or may not have been a "trick", but enormous poll location lines do tend to have that effect.

Pima County opened fractionally less than 50% of their locations. This trend away from polling places in Maricopa and a 34.8% poll location rate deserves an explanation.

3. Operations, Security And Transparency At The Central Tabulator

The following map of the central tabulator operations facility is by Jim March.



The drawing above represents a small part of the operation during election night. For the most part the observers and security cameras do not see what going on in the warehouse where the memory cartridges are coming in and the other areas of the building pre-processing provisional and mail-in votes. In the map, the warehouse is a huge room accessible by doors 2 and 3 (lower right and left) while offices processing provisionals and mail-in votes (checking signatures and voting status) are in offices beyond door 4 (top left).

4) Networking And Data Interchange Security.

There are eight scanners wired via Ethernet networking to the same small (allegedly) “disconnected” network used only for election processing and not cross-wired to the county's internal network or the Internet.

No effort was made on election night to prove this, despite a mildly-phrased request to do so.

According to the election department's IT manager Mr. John Stewart, at least one printer was on this network along with the central tabulator. We then counted the cables coming out of the hub and up into the ceiling and found one extra cable. A query showed that this “extra” cable went over to a standard PC on the opposite end of the facility, allegedly to allow that system to print to the same large laser printer the voting systems share. In the map this is referred to as the “mystery PC”.

The cables vanish into the ceiling and then come out at key points.

Vote totals are allegedly transferred from the eight scanner stations to the central tabulator (room at the

far left in the map) **by USB memory stick devices**. The mail-in vote totals were transferred to the central tabulator by memory stick approximately mid-day on election day (Feb. 5th).

After the polls closed we observed USB memory sticks in action – transferring data from the central tabulator (vote totals) to a PC that is directly wired to the Internet to upload results to the county's website. This was the origin of the vote total reports beginning at 8:09PM that culminated into the final election results report. When the memory stick had performed this task, it was brought to a laptop where it was re-formatted in front of observers before being stuck back in the central tabulator for the next batch of upload data.

On election night results are uploaded by modem from the precincts.

Concerns:

4a) When these cables vanish into the wall, they can go into a splitter (hub) and from there to another PC that can subvert the election, taking remote control of the databases in any of the central systems. Equally troubling, such a concealed connection could lead to the Internet itself. It is impossible to overstate the ease with which this "hardware hack" could be accomplished. A laptop set up to monitor all communications would capture all of the print jobs of vote totals a week or more pre-election, allowing a "data thief" to read how the mail-in vote is progressing pre-election (a felony). These printouts are needed, but they get boxed up and locked away un-viewed with batches of mail-in votes that can be hand-audited later. A laptop set to monitor the print communications could upload stolen data via a cellular-network modem on an untraceable signal. These cell-modem cards are common, sold by Verizon, Sprint, AT&T and the like for less than $150.

Suggestion: ALL data interchange cables associated with or connected to the voting system must be eyeball-visible their entire length.

1880 Equivalent Situation: if a special hallway or tunnel was constructed to carry votes, and was not allowed to be observed nor the time in transit paid attention to, fraudulent alteration of the paper votes could happen. A failure of observation of this sort wouldn't be tolerated. When the data passes over Ethernet disappearing into ceiling panels, there is no practical difference.

4b) The "mystery system" contains uncertified software and isn't checked out in the Logic & Accuracy testing (see right area of map). *Update: we now know it was running BPS/Bridge – see Appendix A.*

Suggestion: no system not tied to the election process *(or certified – see Appendix A!)* can be allowed to be connected to the voting system.

1880 Equivalent Situation: picture a ballot box on a table. Picture a curtain around the table. Picture a hole in the top of the table and bottom of the ballot box. *Put a midget (err, "height challenged individual") behind the curtain.* This is the actual implication of having an additional system tied in – it's connection can be used to pump data into the database that holds the real ballot box, electronically.

4c) The scanner stations are allegedly connected to the central tabulator network wiring "only for

printing". The cross-connection to the central tabulator could allow "data theft" of the sort encountered in Pima County, where reports of mail-in voting results from live ballots on a precinct detail level have been raided regularly since the 2004 primaries. Either give each scanner station (or pair of stations) their own small printer, or give them their own small network with openly exposed cables running purely to a printer.

Suggestion: if the scanner stations need to print, fine, wire them up to their own printer, best yet one small laser printer each and avoid networking altogether. Per the department, networks aren't needed.

1880 Equivalent Situation: not applicable...the analogy just doesn't stretch here because they'd have "strung up" anybody who seriously suggested such a thing...

4d) Transferring election data on the memory stick to the "internet reporting computer" (see diagram) provided the appearance of an acceptable level of security. This appeared to provide observable, physical evidence that the election system was not cross-wired to the Internet.

But formatting the memory stick before each pass, thus clearing its memory for each reporting period, destroys any chance at knowing the continuity of the data from each transfer across election night.

Had they burned CD-ROMs with the out-bound data at the central tabulator, they could have marked each CD and kept a continuous "fixed" electronic record after the transfers. CDs cannot be changed once initially burned – USB flash memory certainly can. (The results of 2/7/2008 at 3:37:41 PM reflect this problem. The additional 45,503 votes per Randall Holmes (DEM Observer) are early votes. Early ballots, aka "vote by mail" or "VBM", were run but not put in the proper category of early votes. Instead, they were put in the overall totals giving the impression that they were votes cast at precincts.) With the USB flash memory device re-written each pass, the previous record of what was transferred to the Internet is gone forever. Also troubling: it would be an admittedly very advanced hack, but the re-format process on the laptop in the middle could have written malicious code to the flash drive before it went back into the central tabulator. Is this likely? No – you'd have to write a disk formatter with a booby trap that looks like the real Microsoft utility. There were less than a dozen reports on election night, and since blank CDs cost about a quarter each, burning CDs instead of using memory sticks doesn't seem an unreasonable concept.

Suggestion: CDs cannot be changed once initially burned – USB flash memory can. CD-ROMs should be used to transfer data from the central tabulator to the internet reporting computer to allow for continuity of the data to be retained. This practice would aid in later auditing or verifications of data continuity, security and authenticity. Each CD would be labeled as to date and time then filed securely.

4e) Allowing precincts to upload results by modem opens security holes. In theory a precinct might upload results to the wrong number coded in by a malicious poll worker, and the "man in the middle" attacker would alter results and pass them along to elections HQ. More seriously, the modems form a line of communication from the outside world into the central tabulator for any hacker that has the phone number, including at least some poll workers and election staff and possibly some vendor staff.

John Brakey witnessed several single individual deliveries of the memory packs to the front office. Most

of these people were sent to the back of facility which is out of sight of the Party observers.

Suggestions: Turn off the modems and standardize (with observation procedures) the memory pack transfer process into the elections office HQ (central tabulator station).

1880 Equivalent Situation: the modem transfer process is inherently secretive. An opening from the outside world to the ballot counting process is an open avenue of ballot stuffing and/or manipulation. We wouldn't have tolerated it back then with paper and we shouldn't now with electronic data.

5) Visibility And Transparency

Concerns:

5a) Access to the central tabulator is wide open to numerous people when observers are not present. The central tabulator room also contains what appears to be at least one person's office cubicle, and a large selection of cables, "extra parts", manuals and other seemingly extraneous miscellaneous parts. There is no effort made to secure the smaller central tabulator sub-room (left edge of the map) once observers leave. The equivalent to this smaller room in the Pima facility is a vertical cage the size of an old-fashioned phone booth with a door that is both locked and sealed during election processing when observers aren't present. The local network connections are pulled before this "cage" is sealed. The same could be done in Maricopa by sealing the whole smaller room at a minimum when the election is in progress and observers aren't present. By comparison, Pima County provides a camera and a clear view from the public observation location. In Pima County, during the election period the central tabulator systems are locked in a cabinet when not in use, with all data cables disconnected and the case tamper-sealed. Observers record the seal numbers and when processing starts back up observers watch the unsealing. Computer operations cannot happen without observers.

Suggestion: The Maricopa central tabulators can be put in a similar cabinet as Pima uses, or the entire central tabulator room can be sealed during election processing while disconnecting the visible cables.

1880 Equivalent Situation: Don't let anybody tamper with ballots without outside observation.

5b) The smaller central tabulator area is a "no go zone" for observers (see map, left side). Reading the screens is impossible for the naked eye and when we attempted to use a pair of binoculars, county elections staff (primarily Karen Osborne) became verbally abusive and threatening. The binoculars were owned by a member of the Democratic Party's observer corps (Mr. Randall Holmes) who (along with others) later informed me that binocular observation was commonly allowed in previous elections – which is why he had them. Either Osborne changed the policies for this election, or she had a personal grudge against the Libertarian observation team after losing the emergency court hearing that allowed us in over her objections.

The standard in Pima County is to use video signal splitters and extra monitors to show observers exactly what's going on at the central tabulator, on extra screens positioned specifically for observers.

Suggestion: Provide monitors outside the central tabulator room linked to each monitor in the central

tabulator room so observers have access to the same data on the computer screens in real time.

1880 Equivalent Situation: This is about whether or not people can watch the process. The process now happens on computer screens, so observation must now follow to the displays.

5c) We also saw activity in the central tabulator room after the rest of the observers were gone. It was brief, one person moving from one scanner station to the next doing something brief and then going into the central tabulator room each time. This occurred right after the official observers had left. Jim March was still present outside and was able to record this on video through the window from the public observation area (top right corner of map).

*This is the same situation and solutions as 5**a** above.*

6) Mail-in Vote Handling.

Apparently the whole process has been outsourced to a private corporation called Runbeck Election Services. Runbeck prints the ballots, mails them out, takes them back in, scans them and then passes them to the county elections office. We won't do a "concerns" set of bullet points because we believe this outsourcing of a critical elections process is a grave and critical "concern" that will clearly require more detailed and in-depth discussion. Both the practices and the perceptions of integrity of the elections processes must be assured "to even the most casual observer" in order to build confidence in elections.

Suggestion: this is a government function that should be taken back in-house.

7) Outsourcing of Central Tabulator Operations.

The processing of the vote at the central tabulator room was mostly handled by Sequoia employees. Operations at the central tabulator station itself was mostly run by Sequoia employees, including the woman filmed by Jim March active in the room after official observers went home.

Suggestion: this is a government function that should be taken back in-house. If the voting system is too complex to operate in-house, that's a reason to scrap it. See Appendix A for legal grounds to do so.

8) Disturbing Pollworker Reports.

The poll workers we've interviewed have noted high numbers of provisional ballots (as much as 1/3 of the overall precinct vote) in this election. They fall into 3 specific and one general category:

a) "I'm independent but I want to vote anyway!" - estimate of 25% of the provisional ballots cast.

b) "What do you mean I'm a mail-in voter?" - estimate of 50% of provisional ballots cast.

c) "I'm a registered Democrat" (or Republican) but they were listed as other party (or no party) - estimated 25% of the provisional ballots cast.
General: The most visible general problem included long lines, a shortage of poll workers, and the size of precincts that contributed to the running out of Provisional ballots - troubleshooters were making ballot copies at Kinkos Copies on their own dime hoping for recompense later.

Linda Brown with the Arizona Advocacy Network (www.azadvocacy.org) states that on election day her precinct observer program estimated between 10,000 and 50,000 voters disenfranchised.

During Election Day the running dry on provisional ballots was attributed to independent voters by Maricopa County elections officials. Maricopa County officials alleged independent voters demanded to vote regardless of being informed their votes would not be counted. Overall this looks not to be the case.

In the former case, it's understood that their vote won't count. The county elections staff is estimating that these are the bulk of the provisional ballots cast.

The poll workers we've talked to say otherwise, guesstimating these are no more than ¼ of the total provisional ballots cast. The rest were people who didn't think they were mail-in voters as identified as such in the poll worker rosters. See notes below.

- Maricopa County ran 397 precincts out of 1142, a percentage of 35%.
- The total eligible voting base of Democrats and Republicans in Maricopa County was 1,114,208. This breaks down to about 2,807 voters per precinct on Election Day 2/5/2008.
- Pima County ran 200 precincts out of 409, or 48%.
- The total eligible voting base of Democrats and Republicans in Pima County was 335,108. This breaks down to about 1,675 voters per precinct on Election Day, 2/5/2008.

Some voters may have accidentally signed up for long-term mail-in voting. But still, the numbers seem high (as of 2/7/2008 60% of the vote counted is VBM a new record high) and the County's blaming it all on independents voters seems odd. **This is all very preliminary on everybody's part but it bears further scrutiny.** We'll look again once the official provisional totals are in, and see also Appendix B where Mr. Shelby goes into more detail on this issue.

Suggestions withheld on this point pending further research. See also Appendix B.

9) Physical Access Security

Referring back to the map, doors 1 through 4 required card-key access that recorded who entered and exited the facility. But door 5 has no such recording capability: it is accessed by a code sequence shared by multiple users. Adding another card-key recording panel to door 5 is an obvious fix that shouldn't even need comment.

Suggestion: Provide an additional card-key terminal at door 5.

10) Party Access To The Oversight Process.

The authors note that the Maricopa County Elections Department attempted to obstruct the rights to election observation and oversight. The county elections department initially denied computer specialist Jim March and election activist John Brakey credentials as official public observers of pre-election logic

and accuracy testing of the county's electronic voting system. Election department staff and attorneys claimed that credentials would not be accepted via any party for March and Brakey; various excuses were floated including a single 37-year-old non-violent drug conviction on Brakey's part and a claim that March is a "mercenary" for his role in the California consumer protection lawsuit against Diebold.

The only way Jim March and Michael Shelby could get in as Libertarian-credentialed observers was by an emergency court order filed by the Maricopa Libertarian Party supporting the right of ALL parties to conduct election oversight. We would like to thank the chair of the Arizona Libertarian Party, attorney Michael Kielsky for his timely court filing (and win).

Brakey and March were the lead investigators in a recent successful public records lawsuit against the Pima County Elections Department which resulted in the release of 300 election databases, the largest release of raw election data in the history of electronic voting. They have twice found illegal, uncertified software in the Maricopa elections office (MS-Access, late 2006 and early 2007). March, Brakey, and Shelby are supported in their insistence that "voting is secret, but the counting is public" by Arizona Revised Statute 16-601 – Tally the vote – which states, "The count shall be **public**, in the presence of bystanders." Security of protecting the vote must be a high concern to all.

Suggestion: Maricopa County's elections department must **encourage** oversight, and above all not try to exercise their own discretion in what is clearly a statutory, non-discretionary situation. The county cannot try to control who does oversight and observation: not legally, not morally.

Comments And Conclusion

This agency has "upgraded" their voting system to the electronic age. They must therefore genuinely upgrade the observation process to the same level or above, or provide an open invitation to fraud. This means addressing the suggestions in this document: full public records access on a timely basis, open and visible cabling, the elimination of non-certified systems from the voting system network, a willingness to allow immediate spot-checks of connectivity issues and more.

Above all, a "cultural shift" is needed: the county elections office must become determined to prove that the process is fair, rather than the current practice of hamstringing observation at every step.

Let us explain why Maricopa County should voluntarily support the changeover.

Every once in a while, an election "blooper" happens. The most recent comes from New York City. In precincts with the highest African-American population rates in the US, Presidential candidate Barack Obama received zero votes. This falls into the category of "impossible results" and was soon corrected. In a situation like this where the appearance of fraud is downright glaring, the ONLY thing that can salvage the election division's credibility is transparency. It's not possible to pretend nothing is wrong; salvation lies in total transparency. If this glitch had happened in Maricopa, the county couldn't prove it wasn't fraud under the current level of "observation" seen by our team in this election. As it stands, the GOP vote pattern discrepancy between mail-in and precinct voting alone raises questions.

When an even more serious "impossible result" happened in Sarasota FL in 2006, the county's process

and their ES&S systems could not show what really happened. Public trust in that agency is still shattered. *To run a non-transparent election and hope no serious glitches occur is much like driving without insurance – you can get away with it for a while, but it's both illegal and a bad idea.*

Instead of running a transparent process, Maricopa County has put the appearance of security over the actuality.

Worst of all is the out-sourcing of huge chunks of the process - mail handling on both incoming and outgoing ballots to Runbeck, and central tabulator operations to Sequoia. The conflict of interest borders on horrifying: should anything go wrong with the Sequoia voting machines as one example, the Sequoia employee operators of those systems will be under tremendous pressure to cover up the issue. We have a copy of a Diebold manual on employee field operations marked "not for customer review" which baldly states: "employees will not discuss shortcomings of our products, even where obvious." We see no reason Sequoia's staff will operate any differently.

At the conclusion of the election, party observers were invited to sign that they had indeed observed the election. March and Shelby did not, because they considered it perjury to do so under the circumstances created by the Maricopa elections department.

We don't think the elections department themselves are any more qualified to state with certainty what really happened with this election.

It doesn't have to be this way. The trend in Arizona legislation is to lay out principles in broad strokes. The "broad stroke" in this case is "elections will be observed".

The legislature hasn't filled in the "electronic observation" detail. We don't think they need to. The election process is either run in secret or it isn't. This election was run in secret.

We submit that this was illegal on it's face.

Appendix A
The Sequoia Voting System Installation in Maricopa: A Legal And Practical Analysis

Maricopa County is the largest client county Sequoia has, and is a fairly recent installation (mid-2006).

There are a number of intersecting concerns related to the security and legality of this system. Public records access in the course of producing this report has left the authors in the best possible situation to comment. We will draw heavily from the security analysis published last year pursuant to the California Secretary of State's "top to bottom review" and legal analysis performed by Dr. Tom Ryan in Arizona.

We will however be able to go past where these and other pioneers have left us.

Legal Background

Voting systems in Arizona are certified by the Arizona Secretary of State's office, with a limitation placed on her powers:

> 16-442.B. On completion of acquisition of machines or devices that comply with the help America vote act of 2002 (P.L. 107-252), machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with the help America vote act of 2002 and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to the help America vote act of 2002.

The Help America Vote Act further codified an existing system of Federally approved test labs which are the sole people outside of the voting system vendors who are allowed to peer into how these machines work: taking them apart with screwdrivers and more importantly, reviewing the "source code" behind their functionality. This lets the labs (in theory) check the products for accidental "glitches", various security flaws and worse, deliberate "fraud logic".

In order to allow Maricopa County to do their own ballot preparation (electronic and paper ballot layouts, Sequoia sold the county a software module called "BPS", which includes a data-transfer program to load BPS information into the main Sequoia elections database called the "Bridge Tool".

Sequoia, recently supported by Arizona Secretary of State Jan Brewer, is claiming that the BPS/Bridge software components don't need to be Federally certified per the Federal rulebook (2002 edition) covering the test process.

The authors of this report think otherwise. We believe Sequoia deliberately withheld BPS/Bridge code from outside review that is critical to the operation of the election, code that is central enough to the functionality of the system to subvert or corrupt the election process. Per the Federal rulebook, they required test lab review.

Further, our reading of 16-442.B as a limit on the AZ SecState's powers removes her discretion in this matter. Factually, the code either needs certification under the Federal 2002 rules or it doesn't. If it does, and per admissions already made it hasn't been, then due to the Federal rules making the entire voting system certified as a complete unit, the whole collection of Sequoia parts from the precinct terminals back is legally *not a voting system*. It's as fake as a Hong Kong Rolex.

The Federal Legalities

Per the Federal 2002 Voluntary Voting System Standards rulebook[1]:

> 1.5.1 Voting System
>
> A voting system is a combination of mechanical, electromechanical, or electronic equipment. **It includes the software required to program, control, and support the equipment that is used to define ballots**; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. A voting system may also include the transmission of results over telecommunication networks. [Emphasis added]

Sequoia's "BPS" product prepares the electronic and paper ballot layouts, formats them and inputs the data into the main database of votes (controlled by a certified program called "WinEDS"). Depending on which Sequoia document you look at, "BPS" stands for "Ballot Preparation Software", "Ballot Production System" or a couple of other variants[2].

Sequoia's usual business model is to do ballot prep in-house as a service to client agencies; Maricopa is one of a very few who fought that idea and were offered BPS/Bridge as licensed products to do it themselves. It seems possible the Sequoia salespeople who sold them BPS didn't realize they were releasing a legally questionable product to outside scrutiny. Note that BPS/Bridge is active in the election process no matter who uses it at what office; the availability of BPS in the Maricopa elections office doesn't affect it's legality either way. It does give us the opportunity to examine the situation.

AZ SecState Jan Brewer says (in a letter of 2/7/08):

> A "voting system" is defined in Section 1.5.1 of the VSS to generally mean the total system used to define the manner in which ballots are cast, counted, reported, maintained, audited and tested. BPS is a stand-alone system that enables the user to layout ballots and then import the information directly into the WinEDS program. The WinEDS program is the certified election management system used by Sequoia.
>
> So long as the management system that actually creates the ballots is certified, then the 2002 VSS do not require a stand-alone system that supplements the ballot layout process to be separately certified. To the extent there are references in the 2002 VSS to ballot preparation systems, these

[1] "Voluntary" means the states don't have to adopt it – Arizona along with 37 other states has by statute so there's nothing "voluntary" about it for us.

[2] They're either obfuscating what software is being used/shipped, or their marketing department needs to hire an editor...

> references refer to ballot preparation systems that are integrated into the election management system itself. I will note that Maricopa County has successfully used the BPS now for several elections, including the 2006 primary and general elections.

So let's define the term "Integrated Software System"

> "A system in which separate programs perform separate functions with communication and data-passing between functional programs performing standardized I/O routines and a common data-base." - http://www.pera.net/Tools/Glossary/Enterprise_Integration/Glossary_I.html

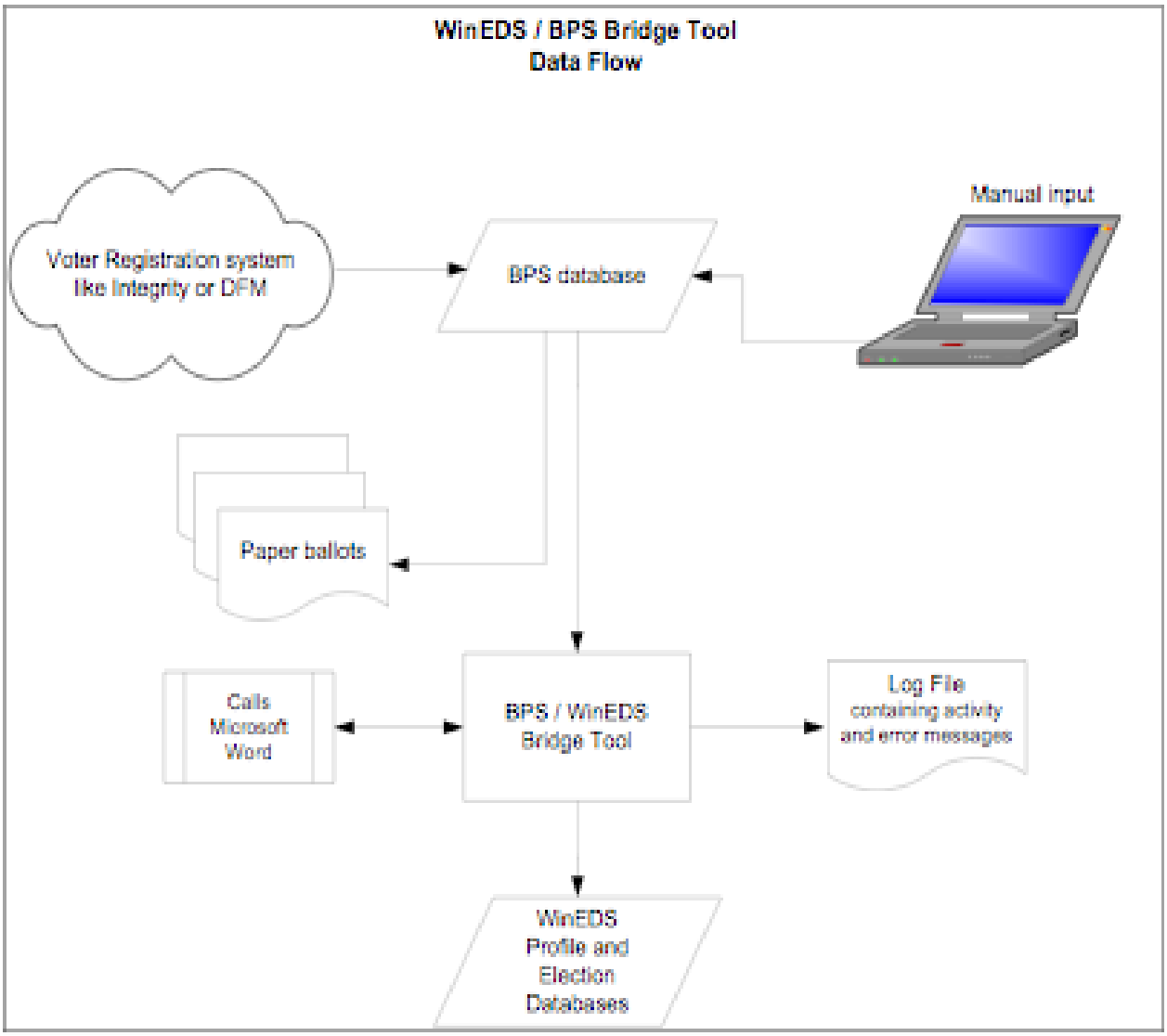
As Dr. Ryan puts it:

> "An integrated system is a collection of subsystems that might include many "programs" and hardware devices. In the case at hand, the integrated election system is not just the WinEDS program. It includes scanners, touchscreens, modems, memory cards, all election-related software, ballots, etc. These are supposed to be tested by the ITA as a single system."

The Federal Election Assistance Commission has given a preliminary opinion (Brian Hancock in a letter of February 19, 2008):

> My understanding is that BPS is an optical scan ballot formatting and typesetting program. It also has the ability to input and manage candidate filing. The outputs of this program are inspected by election officials to ensure that correct geographical boundaries, candidate and contest information, spelling, etc. are produced. The bridge is described as a software utility that provides one to one mapping of information from the BPS database to the WinEDS election management system. This mapping function is also checked by election officials.
>
> It is very clear that voting systems seeking certification and incorporating these functions would require testing of these components under the 2005 VVSG. He goes on to say that the definition of voting system is not as clear in the 2002 standards so they haven't required certification of the BPS or the bridge.

BUT we also have some Sequoia manuals on this subject, including this graphic of theirs:



As you can see, ballots are prepared based on manual input ***straight into the BPS database*** using input from the voter registration system and straight to paper with no intervening process. Data from BPS also drops into WinEDS by way of the "Bridge Tool" module (center) distributed with BPS.

At this point referring back to the FEC 2002 standards just seals the matter:

> **Vol. I. Section 9.4.1.1. Focus of Functionality Tests**
>
> The ITA designs and performs procedures to test a voting system against the requirements outlined in Section 2.
>
> ---
>
> **1.6.1 Qualification Tests**
>
> … Qualification tests address individual system components or elements, as well as the integrated

system as a whole.

Section 2. Functional Capabilities

Section 2.1 Pre-voting Capabilities: These functional capabilities are used to prepare the voting system for voting. **They include ballot preparation**, the preparation of election-specific software (including firmware), the production of ballots or ballot pages, the installation of ballots and ballot counting software (including firmware), and system and equipment tests. [Emphasis added]

6.2.1 Testing Breadth

ITAs shall design and perform procedures that test the voting system capabilities for the system as a whole.
---
9 Overview of Qualification Tests
9.5 Test Applicability
9.5.1.2 Software

Specialized software for ballot preparation, election programming, vote recording, vote tabulation, vote consolidation and reporting, and audit trail production shall be subjected to code inspection. Functional testing of all these programs during software evaluation and system-level testing shall exercise any specially tailored software off-line from the ballot counting process (e.g.; software for preparing ballots and broadcasting results). [Emph. added]

Section 2.3.1 Ballot Preparation

Ballot preparation is the process of using election databases to define the specific contests, questions, and related instructions to be contained in ballots and to produce all permissible ballot layouts. Ballot preparation requirements include:

General capabilities for ballot preparation;
Ballot formatting; and
Ballot production. [Emphasis added]

Clear so far? We'll add one more snippet of the 2002 standards by which the Maricopa installation was tested:

4.1.3 Exclusions

Some voting systems use equipment, such as personal computers, that may be used for other purposes and have resident on the equipment general purpose software such as operating systems, programming language compilers, database management systems, and Web browsers. Such software is governed by the Standards unless:

The software provides no support of voting system capabilities;

> The software is removable, disconnectable, or switchable such that it cannot function while voting system functions are enabled; and
>
> Procedures are provided that confirm that the software has been removed, disconnected, or switched.

So: if there is such a serious disparity between Brian Hancock's position on this from the EAC and the EAC's own "rulebook" (2002 edition under which the current Sequoia gear was tested), we have to ask "would the EAC ignore credible evidence of a vendor's serious misconduct?"

The answer appears to be "yes".

On May 11th 2007, Black Box Voting went public with allegations of certification misconduct against another vendor, Advanced Voting Solutions:

http://www.bbvforums.org/forums/messages/1954/47342.html

This article was backed by a series of leaked photographs showing AVS "Winvote" machines with radically different hardware "innards" shipped into the field:

http://www.bbvforums.org/forums/messages/73/differences_in_machines-44965.pdf

Before this article was published, Black Box Voting board of directors member Jim March walked into the EAC's Washington DC offices and personally delivered printouts of the pictures shown in the PDF link directly above. Variances in system hardware was not legally possible because AVS had only one certification number ever issued, for one set of election hardware components.

This report was completely ignored by none other than Brian Hancock. If the FAA was presented with pictures of the innards of a Boeing 747 in passenger service with fake parts, it would be grounded and an extensive investigation launched. The EAC showed no such professionalism.

A few months later AVS needed to do some supplemental software certification with a newly authorized test lab, iBeta. To their credit, iBeta (despite their primary business being the testing of *video games*) took one look at the hardware, compared it to the authorized parts manifest and blew the whistle. The EAC had eagerly ignored community complaints about this vendor but could hardly do the same when one of their test labs said the same thing.

The scandal finally broke in August 2007 as various memos show. Go to this page and look up "AVS":

http://www.eac.gov/voting%20systems/voting-system-certification/registered-manufacturers/

The "correspondence" section is interesting but the bottom line is in the link marked "Applications Terminated" - AVS is officially out of the vote biz as of 11/28/07 and the contact phone numbers at their website are all dead: http://www.advancedvoting.com/index.php?p=Contact+Us

The attitude of the EAC in general and Brian Hancock specifically is clear: if a complaint about a vendor

comes from anybody other than the agency or their labs, it is ignored no matter how obvious.

So What Is The Actual Impact?

This issue isn't just theoretical. We now know the volume of data being "pumped" into the certified voting system components (WinEDS) from BPS from public records – a directory listing of the BPS station:

```
01/11/2008  01:10 PM        22,110,913 AZ08JAN112008A.zip
01/14/2008  08:59 AM        22,110,913 AZ08jan142008a.zip
01/25/2008  03:35 PM        24,797,280 AZ08JAN252008A.zip
01/11/2008  01:10 PM        53,309,440 AZ08Prep.mdb
01/25/2008  03:30 PM        70,529,024 AZ08Tbls.mdb
02/05/2008  04:45 PM        63,971,328 BpsApps.mde
```

This is just the data covering the election of Feb. 5th 2008. The **smallest** of these files is 22 megabytes. The biggest is over 70. This is a lot of data being generated by a program that nobody outside of Sequoia knows anything about. (The 70.5meg file is the most likely data set transferred.)

Let's assume your humble authors were election consultants. We were preparing data for Maricopa County and it was being pumped into the certified election system – files of this size that were created by code only we knew the innards of.

The county elections office would rightly panic. Yet they "trust this vendor".

Why Did Sequoia Commit Certification Fraud?

We have a series of Email communications between Sequoia and the county in which Sequoia asks about the hardware and software environment that BPS is running in:

> From: Elder, Randy [mailto:relder@sequoiavote.com]
> Sent: Monday, October 29, 2007 3:42 PM
> To: Eliza Luna - RISCX
> Subject: BPS Survey
>
> Eliza,
> In order for us to better understand the various machine configurations that are currently being used on your BPS computers; please provide the following information about those systems: If you have more than one computer please provide a set of info for each of the systems being used for BPS processing or BPS database maintenance.
>
> Hardware:
> Manufacturer/Model:
> Processor speed:
> Memory:

Operating System and service pak:
Office Release and service pak:
Visio Release and service pak:
Acrobat Version:
BPS version and date from startup form:

This information will help us in supporting you in the upcoming elections. If any updates are recommended for these products we will contact you to coordinate those changes.

Hope everything is going well.

Randy Elder
Product Development Manager BPS
Sequoia Voting Systems
1705 Chitwood St.
Benton, AR 72019
o:(501) 776-2390
f: (501) 776-2628
m:(501) 765-8479
relder@sequoiavote.com
www.sequoiavote.com

Problem: Neither Visio or Microsoft Office are certified voting system components. MS-Office includes MS-Access, which is widely understood to be a security nightmare able to hand-manipulate the databases BPS is passing to WinEDS. Refer back to the directory listing: ".MDB" and ".MDE" file extensions are Microsoft Access data files open to manual or automated (Visual Basic script) manipulation.

In other words, it's not just that BPS isn't certified and therefore Sequoia has committed a technical violation of the Federal rules. ***It can't be certified as it relies on components no test lab in their right mind would approve,*** especially since two out of the three original test labs have been throw out of the process for poor performance (Ciber and Wyle).

In 2006 John Brakey and Jim March examined the Maricopa Sequoia installation briefly and found Microsoft Office (including Access) installed on the central tabulation system. We were told that it's presence was accidental, part of the "standard applications" the county installs on every machine.

In early 2007 the Democratic Party held their annual convention including elections of officers, on Sequoia voting systems provided by Maricopa County. Yet again, MS-Access was present, spotted by Jim March. Yet again, the county passed this off as an accident.

They lied both times. BPS requires the presence of MS-Access.

For the sake of completeness here's the county's response to Sequoia's query:

From: Eliza Luna - RISCX
Sent: Wednesday, October 31, 2007 8:01 AM

To: 'Elder, Randy' Cc: John Stewart - RISCX
Subject: RE: BPS Survey

Hardware:
Manufacturer/Model: Dell Precision 490
Processor speed: 3 Gig
Memory: 3 Gig
Operating System and service pak: XP Pro SP2
Office Release and service pak: Office 2003
Visio Release and service pak: Visio 2002
Acrobat Version: 5 Professional
BPS version and date from startup form:3.40L3 8/28/07

Conclusions:

- Sequoia withheld a major portion of their voting system product line from all outside scrutiny.

- They likely did so because this module depended on known insecure sub-components (especially MS-Access) and allows easy manual manipulation of the data it produces. MS-Access also likely allows hand-editing of the core WinEDS database containing votes as Access can manipulate SQL data on which WinEDS relies.

- Three government agencies are covering this fiasco up – the Federal EAC, AZ SecState and the county elections agency.

We have filed a public records request for the actual database files, first from WinEDS and now a second request for the BPS-generated files. The county has replied so far on the WinEDS data that it is the "trade secret intellectual property" of Sequoia. On reviewing Sequoia's actual letter, we sent a response to Ms. Colleen Conner, Maricopa County of the attorney's office that we'll include here as it outlines a potentially bigger problem:

```
Ms. Conner,

Thank you kindly for your public records response provided Friday the 14th.

As you know we have two public records queries outstanding at this point:

* A request for the WinEDS central tabulator databases in ".SQL" format.  Call
this the "SQL request" made in the original records request.

* A request for the raw .MDB files known to be generated by the BPS software
module, which I'll refer to in shorthand as the "MDB request" we filed later
by EMail.

On Friday you provided a paper copy of a Sequoia document claiming trade
secret protection on the SQL request - for the convenience of those CCed I've
scanned and attached this document.  In that letter, Sequoia claims to be
embedding "software" within the SQL files.  This is an unconventional practice
at best and raises questions beyond the scope of simple records requests.  As
```

you know, voting system software in Arizona cannot be certified by the AZ SecState's office unless it's been federally certified first. The Federal certification process includes a ban on interpreted code, and a requirement that the federally approved test lab take a "hashed snapshot" of the working code they test. That latter means it is possible at any time to mathematically prove that executable code in the field in Maricopa or elsewhere matches the mathematical "pattern" identified by the lab - proving that the two code sets are identical internally no matter how far removed geographically or in time.

However, for this "hash code checking" to work, the software must be contained in files that don't change over time.

Sequoia's claim that they've embedded election software in data files that vary by jurisdiction and election is therefore highly troubling. It means they've stripped out a basic protection identifiable in the federal voting system certification rules. It appears at least possible (and I would go so far as to say "likely") that the end result cannot possibly meet the federal voting system certification standards.

The AZ SecState's ability to certify voting systems in this state is conditional on federal certification. There is no statutory discretion allowed under Arizona Revised Statutes 16-442.B:

On completion of acquisition of machines or devices that comply with the help America vote act of 2002 (P.L. 107-252), machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with the help America vote act of 2002 and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to the help America vote act of 2002.

In other words, without even getting into the subject of BPS, Sequoia appears to have identified a whole new way in which their product line is utterly illegal for use.

OK. Set all that aside for a moment.

You have told me verbally that you have passed the request for the BPS data (MDB files) along to Sequoia for comment.

My main purpose in writing this is to demand the release of that BPS/MDB data.

Sequoia appears to be taking their own sweet time responding to this request, and I can tell you exactly why.

In the Sequoia letter responding to the request for SQL data dated Mar. 5th '08, they agree that most of the contents of the SQL data that include vote totals, election setup and the like are indeed public, and offer to work with us to segregate that material from the embedded "trade secret software".

They didn't expect the follow-up BPS/MDB data request. They're now stuck: if they claim embedded code in the MDB files, they're admitting an open-and-shut certification violation. We could argue for days about whether or not the BPS

software requires certification; I believe it does and you'll get my full written position on that within days. At present all parties agree on one thing: BPS has not been certified. That means that only Sequoia knows what's really in it, by definition: no independent lab has checked out it's contents. If BPS is injecting code into the WinEDS/SQL "data files" which per Sequoia also contain code, then we've got a REAL mess on our hands, don't we?

I think Sequoia has figured out this degree in which their letter of Mar. 5th paints them into a corner.

In other words, the only possible excuse Sequoia could offer to keep the BPS/MDB files out of my hands would reveal the most extreme violation of certification standards found to date, and that's saying a lot given the known certification violations of other companies.

In conclusion, I would ask you to pressure Sequoia for a response on the BPS/MDB data file request rapidly. I would be willing to bet the request for the BPS/MDB has their tails in serious knots; those files will show the degree of manipulation of the process the BPS module is capable of, which will speak to the fact that it should have been certified...but if they pull the same "proprietary software" gag they're in even more trouble.

Which in turn means I'm not going to let them sit on this forever, since the exact same issues should be obvious to you and your people long before Sequoia even replies.

Since withholding is legal impossible on Sequoia's part, I respectfully ask that you release the BPS/MDB files.

I would also suggest that in light of their claims that the WinEDS/SQL data contains programs, your people (and the AZ SecState's staff) take another look at the actual certification status of the Sequoia WinEDS product. I have no ability to force you to do so short of court action, but I do humbly suggest that you can save yourself significant "egg on face" issues down the road.

Thank you for your kind attention,

Jim March

SEQUOIA
voting systems

March 5, 2008

Colleen Connor
Deputy County Attorney
Maricopa County Attorney's Office
222 N. Central Ave., Suite 1100
Phoenix, AZ 85003

Dear Ms. Connor :

Sequoia Voting Systems is in receipt of the public records and email to your offices from a Mr. Jim March dated February 21, 2008. This letter addresses the public availability of the WinEDS election database as referenced in item 18 of the public records request. Specifically, item (18) requests:

"All central tabulator databases from the central tabulator station, in SQL format – as many as you have, in electronic form ONLY, un-redacted."

Sequoia Voting Systems claims as a proprietary trade secret the election database. The data base contains embedded proprietary software code and proprietary stored procedures, which are also software code authored by Sequoia Voting Systems technical staff members. Sequoia would be harmed if this information were to be viewed by competitor voting systems vendors. It has been our past and current practice to vigorously protect this competitive differentiator and thus must respectfully decline its disclosure as part of this request.

We believe Mr. March's assertions to possibly stem from a misunderstanding of Sequoia's election database structure and the initiation of an election database (which is ultimately placed on the central count server). Unlike other election vendors' products, the Sequoia election database starts from a default structure that is part of the licensed WinEDS software package. The election database is built from the default database. This default database contains the proprietary code described above. Later, as geographic, polling place, and other information is input to the database, the default database evolves into the election database for a particular jurisdiction and a particular election within that jurisdiction. Therefore the unredacted election database is not a public record.

Notwithstanding and in the interest of cooperation and providing a meaningful response, Sequoia Voting Systems will make available, in electronic format, the non-proprietary election specific information in the election database, referred to in the public records request as the SQL central tabulator database. We agree with Mr. March's comment that this portion of the database, containing the data specific to the Maricopa County election of February 5, 2008 is a public record and should not be withheld. This in no way affects the validity or enforceability of our position relative to the proprietary nature of those portions of the database previously outlined.

Moreover, by providing the election specific data but not the proprietary portions of the data, interested parties can utilize third party database analysis tools such as AdeptSQL to analyze the election specific data within the election database and could, through use of a tool such as

AdeptSQL, derive audit information. This audit information would typically include: the date and time of data entry, date and time of elections results entry, and Microsoft based security identifiers from individual pieces of data within the database. Interested members of the public could perform an independent canvass of the results by utilizing the election specific (non-proprietary) portions of the database and thus can assess the integrity of the results, without the need to access Sequoia Voting Systems' proprietary information. Finally, the proprietary software code will not aid or further enhance the integrity assessment of an election.

Do not hesitate to contact me to discuss these matters.

Best Regards,

Edwin B. Smith, III

Edwin B. Smith, III
Vice President
Compliance/Quality/Certification

We are going to break through this veil of secrecy, lies and fraud. Too much is at stake to do otherwise. Above all, we want to see what's in those .MDB files and it appears Sequoia is going to have a very hard time denying us those files.

While we would prefer to leave off at this point concluding our own research, at the risk of overwhelming the reader we're going to briefly touch on how much **worse** the situation is.

In 2007 the California Secretary of State's office published a series of reports on voting machines – by far the most complete security analysis documents to date. Separate groups reviewed the disability access features of these systems, their source code, documentation and overall security.

The security testing was in the form of "red team attacks": voting systems were configured as they would be in real life and then "attacked" by professional computer security experts acting from the point of view of both voters and other "outsiders" to the system, and elections staff/vendor staff "insiders".

The systems all failed to at least some degree to "outsider class" attacks and were downright shockingly vulnerable to insider attacks. In most cases (across **all** the vendors) these insider attacks were both possible and either easily concealable or happened without leaving any traces needing a cover-up effort. *America's voting systems were universally found to be obvious targets for data manipulation and vote fraud.*

All of the California top-to-bottom voting system review reports can be found at:

http://www.sos.ca.gov/elections/elections_vsr.htm

Matt Blaze PhD (University of Pennsylvania computer science professor) was the *Red Team* leader investigating the Sequoia voting system for the California SOS Top-to-Bottom Review. Dr. Blaze was asked on Voice of the Voters Radio August 8, 2007:

> Q: "What *is the current condition of all electronic voting equipment in United States of America?"*
>
> Answer: **"*Fatally Flawed*!"** …we're 3 to 5 years before anything better will be available.

In the source code review section of the Sequoia reports linked above (led by Dr. Blaze) we find:

> **3.1.2 Integrity of Precinct Voting Firmware and Software**
>
> The previous section noted ways in which MemoryPack or Results Cartridge data can be subverted after the polls close to introduce false precinct returns into the WinEDS system. In this section, we discuss in which precinct equipment can be vulnerable to tampering before the polls open.
>
> **In particular, the safeguards against the introduction of unauthorized or corrupt firmware**

> **into Sequoia precinct voting hardware are largely ineffective.** An individual with even brief access to polling station hardware can tamper with installed firmware in a way that causes votes and paper trails to be recorded incorrectly, security logs to be corrupted, or ballots to be presented to voters incorrectly. Under some configurations and conditions, corrupt firmware may be able to be spread virally from compromised hardware and may persist across more than one election. [Emphasis added]
>
> The consequences of such attacks can be quite severe and far-reaching; they are largely difficult to detect and sometimes impossible to recover from even if they are detected.

We could cite example after example. From page one of the "red team attack" document for Sequoia:

> In our tests we were able to bypass both the physical and the software security protections of the Sequoia system.

We could pick at random from basically any horror-filled page of the red team report:

> **4.8 Security of the MS SQL Server**
>
> The WinEDS SQL Server is supposed to be a secured, stripped down machine. In the documentation ([10], p. 3-1), it is stated that: "WinEDS currently does NOT utilize code outside of MS SQL Server and no connections or permissions are required on the server (besides SQL Client.) The lack of server access by individual users provides the application with a secure client-server environment. The election data stored on the server can only be modified by authorized users only through the application."
>
> Unfortunately, this is not true. In fact, it is possible to connect to the database and completely compromise the MS SQL server host without using the WinEDS application. This is achieved by exploiting two security problems. First of all, the WinEDS access control procedures can be bypassed. Second, the MS SQL server delivered with the Sequoia system enables users to execute arbitrary commands.

Or we could cut to the last page of the red team report:

> **7 Conclusions**
>
> Although, we did not have enough time to perform a complete evaluation of the Sequoia voting system, we exposed a number of serious security issues. These vulnerabilities could be exploited by a determined attacker to modify (or invalidate) the results of an election.
>
> All the attacks described in this report can be carried out without any knowledge of the source code. In fact, we were able to extract and analyze the Edge's firmware binary representation. In addition, we were able to extend the firmware by using binary patching. This technique allowed us to create a "debugging" version of the firmware, as well as several different "malicious" versions.
>
> The implementation of the attacks did not require access to the source code.

That last is "geek speak" for **"Sequoia vote-hacking does NOT require Sequoia-employee-grade knowledge – any reasonably competent programmer in an elections office could pull it off".**

Now for the punchline: a review of all of the California SecState's material on Sequoia shows they did **not** have access to the BPS/Bridge modules *or even know about them*. All of the security flaws the California test teams found are in **addition** to what we now know about BPS from studying it's manuals and the public records queries performed for this report. BPS creates data in MDB/MDE formats that are far easier to manipulate by hand with **zero** programming skills than what was reported in California.

Sequoia withheld BPS from Federal test lab scrutiny, and because it wasn't in those documents the California SecState's team had no way of knowing about it. This was hardly their fault. **As far as we can tell, all California Sequoia client counties hire Sequoia to do ballot prep. No documents within the California "top to bottom" reports of 2007 give even a hint that the testers knew about BPS[3].**

So as bad as the California teams found Sequoia's security, the situation is far more grim when BPS/Bridge is factored in.

Suggestion: Maricopa County could scrap the system and buy something else. The problem is, everything else on the market is just as bad – the real "core failure" is at the Federally qualified testing labs and the Federal bureaucracy overseeing the labs. Short term, the problems with the Sequoia product line is grounds for increasing the level of oversight, in addition to the dictates of basic sanity and Arizona law.

[3] In 2006 when Sequoia's latest system came up for certification in California, consultant Paul Craft does make very brief mention of BPS and seems to understand that it's involved in ballot preparation. But he does not define what the letters "BPS" stand for and makes no mention of the Bridge Tool, suggesting that he ignored the security implications and likely didn't realize that ballot data was transferred in the easily editable .MDB data format. Leaving all this out bordered on criminal on Craft's part. No mention of Craft's report is found in any of the far more professional 2007 top-to-bottom review documents. California Secretary of State Bowen hasn't used Paul Craft as a consultant at all that we know of.

Appendix B

Report on Permanent Early Voting List Assignments

Michael Shelby

Michael Shelby was one of the Maricopa County voters in the Presidential Preference Primary of 2008 who was surprised to find himself listed as a permanent early voter. Mr. Shelby investigated the practical and legal implications of this confusion which we can state definitively isn't unique to Mr. Shelby.

Following receiving from the City of Phoenix office of the City Clerk Department notification of my inclusion on the permanent early voting list I made inquiry into how my name was on the list.

I have no memory of placing myself on a permanent early voting list. It is, however, just as possible that at some earlier time I did something that put me on the list. The problem is that I just don't know. Until now I had always assumed that the reason I got early ballots before elections was because I vote in all elections and, therefore, maintained my status as an early voter.

My first inquiry was made directly to Karen Osborne during the L&A test observation at MCTEC. Karen informed me, and the assembled others, that the Phoenix Elections Department would have used County records to notify me of permanent early voting and check with them. She indicated that the request form is kept on file as a record for comparison to the voting rolls.

I next phoned the City of Phoenix Elections Department. Their records showed I voted in special elections in 2005 and 2006. They said I must have "checked off the box" that indicated my desire to be put on the permanent list for early voting. I asked if I could see the documentation indicating I had opted into permanent early voting. They said there was none, that their voter records are only retained for 6-months before being purged. They also volunteered how they now utilize the Maricopa County voter database instead of keeping their own. Consolidation with the County database has apparently happened since 2006.

A.R.S. § 16–544 **Permanent early voting list** statutes makes clear that a written request for the purpose of verification of signature is required to be placed on the permanent early voting list. Once verified, the voter is placed on the permanent early voter list that is maintained as part of the voter registration roll. In lieu of the application, a written request that contains the required information can be used. A voter may make a written request to be removed from the permanent early voting list. Again, it must contain the pertinent information specifically the signature of the voter.

I found no provision mandating that the recorder maintain the application for permanent early voting be kept as part of the permanent records. The only requirement is that the recorder add the applicant to the permanent early voting list as part of the voter registration roll.

I found no provision in the statutes to grandfather in permanent early voter lists. Presumably anyone on a permanent early voter list, city or county, prior to November 2007 has been folded into the county recorders office permanent early voter list. It is now up to the recorders office to prove voter intent as to

placement on the permanent early voter list.

Conclusion

In the previous presidential preference primary of those voters who were disenfranchised by not being able to vote or forced into voting a provisional ballot, approximately 50% were reported to have been told they had been sent early ballots. These people were confused and disappointed because they either did not receive an early ballot or had no recollection as to ever having requested an early ballot. The alarming number of provisional ballots cast in this preference primary is cause for significant concern.

Recommendation

The Maricopa County Recorder should send a verification request to every voter now on their permanent early voter list prior to the November 2008 general election. This should be done immediately so as to allow voters to clear up any problems, misunderstandings, or requests to be removed from the list. Unless this is done, there will be a repeat of the presidential preference primary but on a much, much larger scale. This would call into question the competence of the recorders office and the veracity of the election.

To provide an appropriate level of service to the voters and meet its obligations to provide fair elections, the Maricopa County Recorders Office must verify that each voter on the permanent early voter list is aware they are on the list and that they remain on the list until they opt out.

Signed,

M. Shelby

Michael Shelby