



**MISSION:** *We are nonpartisan organization whose mission is to restore public ownership and oversight of elections, work to ensure the fundamental right of every American citizen to vote, and to have each vote counted as intended in a secure, transparent, impartial, and independently audited election process.*

Monday, December 08, 2008 rev 4:06 PM

Chair Rosemary E. Rodriguez  
Election Assistance Commission  
1225 New York Avenue, N.W. - Suite 1100  
Washington, DC 20005

Sent via e-mail to HAVAinfo@eac.gov

Dear Madam Chairwoman and Members of the Board of the EAC:

Now after spending more than 4 years full time understanding how elections work, first in Pima County on Diebold equipment, then in Maricopa County on Sequoia equipment we at AUDIT-AZ can conclude that Elections are unverifiable and are "faith-based" for the most part.

Our Election Integrity Movement in Arizona continues to work to discover more of the flaws built into the election process that been made even more abundantly evident during current general election. It is now time to use all the information that has been gleaned to date to work on solutions to put safeguards in place to assure transparent and auditable counting of the 2010 Election working with Election Defenses Alliance and our other national partners.

The court case in Pima County, Arizona of the Pima County Democratic Party vs. Pima Board of Supervisors set a precedent that the databases produced by electronics voting equipment whether individual machines or in the central tabulators is public record and belongs to the people. With the release of 800 databases this case lead to the largest release of database in the history of Electronic Voting in the United States.

Last July we submitted to the EAC story of Pima County, (Tucson, AZ)

Today we present Maricopa County, (Phoenix, AZ) which is the 4<sup>th</sup> largest county in the United States.

For the sake of keeping this short here are the highlights of what we found and learned:

Maricopa County, AZ Election Department:

- 1) **AS BAD AS DIEBOLD/PREMIER IS, SEQUOIA AND ES&S ARE WORSE!** The equipment Maricopa has was ES&S and in early 2006 converted over to Sequoia. In California ES&S wouldn't even submit their products for review and was disqualified to be used in California.
- 2) **NO SIGNATURES ON POLLTAPES, WHICH AREN'T POSTED AT THE POLLS.** Unsigned polltapes allow the creation of duplicate tapes with fake values after the fact, and are a vital component of any election fraud which seeks to alter both the paper and electronic records of the vote simultaneously.

*Polltapes weren't signed as a matter of county policy and instructions to pollworkers.* Neither are they posted publicly at the polling place on election night to create an independent record of the precinct vote.

Legality: posting of polltapes isn't required in Arizona (yet). But signing them is – the Arizona SecState's election procedures manual carries the force of law. The latest edition (Oct. '07) is online:

[http://www.azsos.gov/election/Electronic\\_Voting\\_System/2007/Manual.pdf](http://www.azsos.gov/election/Electronic_Voting_System/2007/Manual.pdf)

At page 142 we find:

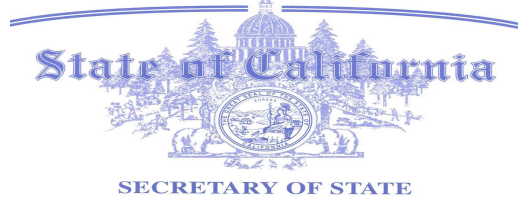
- follow the procedures for printing the totals,
- tear off the tape,
- sign the tape,
- place the tape in the appropriate container or envelope

...

Maricopa county stopped signing the end of day pollworker result tape from the precinct's optical scanner at the same time that the new hand count audit law that we passed in 2006.

- 3) **ATTACKING THE DATA EN ROUTE ("MAN IN THE MIDDLE" ATTACKS).** We learned in Maricopa County election-night that the 22 satellite receiving stations phone modem in the result using a **laptop computer** and that the election results are **not encrypted**. This mentored is **totally prohibited** in California by the Secretary of State. Link to full report:

[http://www.sos.ca.gov/elections/voting\\_systems/sequoia/system40/2008-10-14\\_system40\\_approval.pdf](http://www.sos.ca.gov/elections/voting_systems/sequoia/system40/2008-10-14_system40_approval.pdf)



SECRETARY OF STATE  
APPROVAL OF USE OF  
*SEQUOIA VOTING SYSTEMS'*  
SYSTEM 4.0 VOTING SYSTEM

*"7. No network connections to any device not directly used and necessary for voting system functions may be established, Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time."*

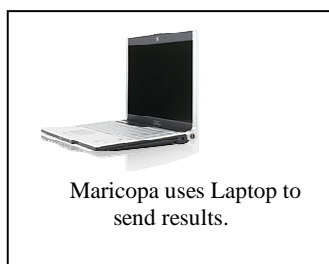


IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 14<sup>th</sup> day of October, 2008.

*Debra Bowen*  
DEBRA BOWEN  
Secretary of State

### Maricopa Vulnerabilities And System Components

#### B.1.5 MPR, MEMORYPACKS, AND CABLES



System Description and Components February 2006 California report.

[http://www.sos.ca.gov/elections/voting\\_systems/sequoia/proposed\\_use\\_procedures.pdf](http://www.sos.ca.gov/elections/voting_systems/sequoia/proposed_use_procedures.pdf)

Excerpt: System Description and Components California Report:

#### Voting Systems

- **MPR:** Is a desktop device, which is plugged into a PC (**usually at the election central site**), and developed specifically to work in conjunction with WinEDS, which is installed on a PC. The MPR performs the following functions (via MemoryPack).
- Burns election data, from WinEDS, onto MemoryPacks, to be used during the election.
- Is used by the Optech Insight to tabulate ballots.
- Transfers the ballot totals to WinEDS, for processing.

- **MemoryPack:** A removable MemoryPack containing the following information is inserted into the rear of the Optech Insight:
- Election Parameter data
- Precinct Totals

The Optech Insight [ed: also used in Maricopa] uses the Election Parameter data programmed into the Memory Pack, using WinEDS to obtain Precinct Totals, during the election.

The MemoryPack may be removed at the end of the election and transported to the Central Counting Location for rapid transfer of Precinct Totals to the Central Counting Location for inclusion into the canvass reports, by WinEDS.

**KEY SECURITY FLAW:** Sequoia doesn't provide a system to modem results from the memory pack reader straight up to the central tabulator. Instead, data is pumped into laptops from memory pack readers at the 22 regional processing facilities, and then the laptops modem results in. First issue is that no independent audit of what Maricopa loads onto those laptops has been performed. We do know that the memory pack data contents aren't encrypted, so "auto manipulation software" at that laptop would be childishly simple to implement. Second, and possibly worse, is that we don't know how many people know the phone number and access codes into the central tabulator station that **receives** those phone calls. Clearly a standard PC can connect in (as that's what the county uses) – could somebody launch a systematic attack on the central tabulator from anywhere in the world? **For all of these reasons and more, California completely banned the use of modems for these purposes as well as Pima County, Arizona.** The rest of the problems we note where seals and ballot box security are inadequate, poll-tapes are unsigned and the hand-audits can be subverted make these problems worse; when combined, these security flaws add up to a total "solution" for vote hacking – BOTH the electronic and paper records can be subverted in lockstep with minimal staff.

**4) MARICOPA HAS A BADLY BROKEN CHAIN OF CUSTODY - MULTIPLE SEALS, ALL THE SAME NUMBER, NO AUDITING OF HOW MANY ARE USED.**

Maricopa purchases their seals in packs of 20 – all 20 bear the same number. At the post-election hand "audit", we observed that the serial number for the seal on both the main ballot bag and the touchscreen "audit" trail pack for precinct Ironwood 400 were 0080400. Other containers holding the provisionals and dropped-off mail-in votes would have been in other containers (the laughable plastic ones pictured) each with two more of these numbers. That's six seals needed. Different precincts received different numbers of seals – some pollworkers report getting 10, or 15, or all 20. According to testimony on a courtroom witness stand under oath by election director Karen Osborne, no check is made of how many unused seals come back in from the field – apparently pollworkers and anyone else involved in handling precinct materials on election night or after are allowed to tamper with ballot containers to whatever degree they like.

We learned of the number of duplicates by accident – the elections office gave their unused seal stash to the county sheriff's office, who used them to secure the lockers that hand "auditors" and observers put our stuff into. Jim March noted that the seals were the same type and same series (starting with "008") as the elections office seals, and photographed a pile of 20-packs. We later confirmed the sheriff's office received these from the elections department.

Legality: this isn't illegal – yet. Nobody ever considered that an elections agency might reject all basic election security processes in this bald-faced a fashion.

**5) A SUBVERTIBLE HAND "AUDIT" PART ONE – THE MAIL-IN VOTE.**

Arizona has a hand-"audit" law, new as of 2006. We fought hard for this law, not realizing that at least where Sequoia equipment is in place, it's useless in "auditing" the mail-in vote.

Here's why. 1% of the mail-in vote is supposed to be "audited". The counties (led by Maricopa) fought tooth and nail to avoid having to sort the mail-in vote by precinct. Instead, counties are supposed to create "audit batches" selected by the political parties. Most of the proponents of the bill were from Pima County and familiar with Diebold gear. In a Diebold-based system,



Here we see dedicated volunteers checking seals on a ballot box, not realizing that a simple centerpunch and hammer renders their dedication absolutely useless.

when you're scanning mail-in votes pre-election the software doesn't track how many votes are in a "batch" of mail-in votes just fed in. So to create an "auditable batch", the system operator (observed by political parties or other observers) prints out a complete "who's winning and losing" report (called a "summary report" in Diebold-speak), scans up to 500 or so ballots, then prints another summary report. Without anybody looking at them, the two summary reports are supposed to be boxed up with that "audit batch" of ballots, sealed away and then made available for hand count later. To get the total votes that should be in the stack, you subtract the first report from the second for any race or candidate. It's clunky but it does work.

Not in Maricopa with Sequoia gear!

Here's how that works: the county scans one of a pre-selected set of "batches" (generally under 200 votes) into the machine, tracking it (like every other such batch!) with their own batch tracking number – as an example, "24-119" might be a valid batch number.

They then box up the votes for batch 24-119 and ask the scanner station computer to print out the vote totals for batch 24-119. The totals are put in a manila envelope, sealed and put in the same "silly box" you can see pictured throughout being center-punched open. Both the county and the political observers note which batch numbers are in which numbered and sealed box, writing down seal numbers.

Spot the problem yet?

After the election but before the "hand-audit", election staff has the ability to ask the computers a critical question: "what vote totals for each candidate or issue are supposed to be in any given batch?"

And that means they can peek into the sealed manila envelope without breaking the seal. *They can produce a duplicate of the report that's in that envelope, after the fact.*

If it's not clear yet: that in turn means they can check to make sure the "audit batches" come out perfectly, covering up either fraud, database glitches or poor quality scanners.

Legality: quality boxes and seals that come from sources that guarantee seal uniqueness would help, but the real cure is to force sorting the mail-in vote by precinct. "Audits" would happen by precinct on a true random pick without worry about "audit batches", printing of pre-election vote totals or any similar stupidity.

## 6) TAMPER-FRIENDLY PRECINCT BALLOT BAGS

The ballot bags holding the main precinct ballot stacks are literally duffel bags of cordura nylon. Instead of the usual zipper lengthwise across the top as in a typical "gym bag", these are cut more square and have a zipper around the upper edge. To "seal" it, a heavy-duty zip tie with a serial number tag connects the two "pull ties" of the standard zipper. It's not that hard to put both zippers near a corner and "turn the bag inside out" enough to get ballots in and out. In the process you'll put stress on the zipper pull-tabs.

DURING THE HAND-"AUDIT" JIM MARCH was able to look at the zippers of about 20 bags. About half were missing the pull-tabs, which were replaced by standard key ring snap-rings.

First issue: were the pull-tabs missing because people were regularly bypassing the seals?

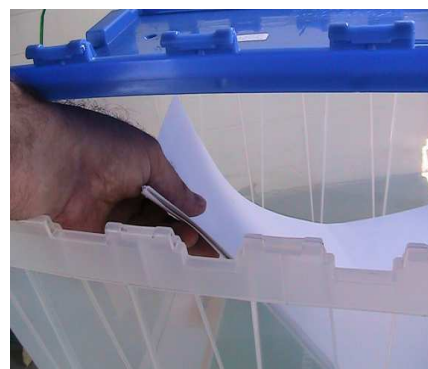


Each side of the box has a single steel "hinge pin" which stays in place due to a "curl" on one end only.



Drive the steel hinge pin out from the end opposite the "retaining curve". The plastic is easily flexible enough to bend around the steel "bump" without leaving a mark.

This "well loved" hammer is worth maybe \$2...



With the hinge-pin removed, it's ballot piracy ahoj, matey...

Note that the pin goes back in as easily as it came out, with zero evidence of tampering.

We've left the "Fry's" price tag intact in case Karen Osbourne tries to clap us in irons for "ballot box theft"...

Second, and even more obvious: once a snap-ring is on there, it can be removed easily in seconds, bypassing the seal. Since this was so common (50% of bags), any ballots you wanted into could have it's pull-tab snipped off with wire cutters and replaced with, you guessed it, a snap-ring as this was the common "fix". *We pleaded with Election Director during the lottery drawing to allow us to put additional seals on the 23 ballot bags that were picked out of the 1,142 precinct ballot bags. Link to audio is below in point 7):*

Physical box security for the mail-in and provisional votes left at the polling places was even dumber – the county uses flip-lid boxes of a very cheap type that are easily opened as pictured.

We found the same exact make/model of ballot box for \$12.99 at the local Fry's Electronics outlet, and tested it's tamper "resistance". It's the translucent box with the blue lids in pictures scattered throughout this document.

Legality: it's actually not illegal in Arizona to use ballot boxes that are tamper-friendly. This will be the subject of urgent legislation this year.

- 7) **A SUBVERTIBLE HAND "AUDIT" PART TWO – THE PRECINCT VOTE.** The morning after the election, the county insisted on immediately having the parties pick the precincts and races to "audit"...even though not all of the initial precinct results were in as required by law. At the moment when they picked the precincts and races to audit, the count wasn't fully "in" - over 300,000 ballots remained to be processed overall including 10 precinct ballot memory packs still missing or not yet reported. Those votes wouldn't be included in any potential audit. Audio excerpts of our complaints that morning are online at: <http://www.youtube.com/watch?v=9oAczDmbWww>

***Legality: they were specifically barred from beginning the hand "audit" process until the entire "unofficial" precinct totals were in and publicly committed.***

Election day was of course Tuesday. The "hand-audit" selection was Wednesday around 9:00am. The hand count didn't start until Thursday morning – across town at the sheriff's Joe Arpaio training facilities who happens to be the most controversial sheriff in the United States. Wednesday afternoon the ballots were moved over to the sheriff's training classrooms, away from camera monitoring for approximately 20 hours until the hand "audit" started.

***THIS WAS BLATANTLY ILLEGAL.*** AZ statutes require holding the ballots under camera scrutiny until they're "audited".

Ballot boxes with dubious security bought on the cheap with duplicate seals available were hauled offsite to offices under the control of the sheriff's staff – the same sheriff who was himself running for re-election in this race, along with some of his key political allies including the county attorney. We have no idea if this triggered abuse, but at a minimum it gave improper appearances.

And all of this was contrary to state law.

Let's recap: would we allow any other candidate's staff to take sole control of ballots for almost a whole day? If the ballot boxes and bags were physically secure with tamper-resistant seals, if polltapes were signed or if chain of custody was otherwise respected we wouldn't be so concerned. With ballots so easy to alter by anyone with physical access, this offsite removal was in our opinion a horrific risk.

- 8) **HOW TO BUILD A BALLOT DUPLICATING STATION THAT FITS IN A CLOSET.**

Maricopa County contracts with a company called Runbeck Election Services for ballot printing and processing. More on them in the next chapter. One of Runbeck's services is the rental of a complete ballot printing "solution" called "Sentio": <http://runbeck.net/?v=sentio>

The idea is that a computer supplied by Runbeck holds encrypted copies of the ballots in .PDF format<sup>1</sup> and prints them to a large Okidata color laser printer "on demand". This seems like a good idea for walk-in early ballots: you don't know what precinct the voter is until they walk in, at which time you print the right ballot for them rather than

---

1 "Portable Document Format", the standard document format used by Adobe Acrobat Reader and other applications.

have stacks of different types and languages. The attached computer is supposed to track how many ballots it prints of each type, as an anti-fraud measure.

The problem is, anybody with the original ballot images (accessible by far too many people) can put them on a laptop, walk up to the "Sentio", unplug the printer from the Runbeck-supplied computer, plug the laptop in, and print an unlimited number of extra ballots.

There would be one risk: the printer has an internal page count, and if somebody "audited" that (tracked how many ballots printed, page count pre-election, page count post...) they might catch the fraud. Well that's no problem. Okidata laser printers aren't hard to find. This one costs about \$6,000 and would fit in a decent-size closet. Smuggle the original PDF ballot image files out on a memory card no bigger than your thumbnail crammed into your cell phone and print as many counterfeit ballots as you want. Runbeck has simply created a blueprint for counterfeit ballot fraud. The ability to make fake ballots makes the day-long visit to the sheriff's offices more frightening – so many of these issues "interact" so that on their own they're of modest interest, together they're a blueprint for fraud.

The only good news is that for some reason, the ballots these Okidata printers generate work OK on a Sequoia scanner but not on Diebold scanners – there was a horrendous failure rate in Pima County and they're likely going to give up on the concept. One theory is that heating the paper in the laser printer's fuser section is stretching it, making the timing marks on the edges fail when Diebold scanners read them. So counterfeiting attempts of this class would be harder in a Diebold county and with more risk of discovery.

## 9) EXCESSIVE OUTSOURCING

Runbeck Election Services prints the ballots in Maricopa County – mostly on big professional offset printers but also using some "Sentio" systems in-house. Mostly normal enough – but they also mail out the ballots to mail-in voters, receive them back in from the voters, scan the signatures, process them by batch for the county and only then ship them off to the county elections office.

The Runbeck mail facilities are monitored by sheriff's deputies, but let's remember the sheriff was running in this election. IF the sheriff is corrupt, finding corrupt deputies would be no problem at all.

At the central tabulator facilities, outsourcing continues. The primary operator for the central tabulator and at least half the staff are Sequoia employees on-site, rather than county employees.

*The level of outsourcing is such that a full vote manipulation could be carried out without a single county elections staffer or officer being involved.*

## 10) SUBVERTIBLE ELECTRONIC BALLOT BOXES ("MEMORY CARTRIDGES")



Recent studies at Princeton University examined a Sequoia voting system of slightly older vintage than what's used in Maricopa. There are however similarities: the "Advantage" pushbutton system in New Jersey runs on a Z80 processor and stores data on EEPROMs – Electrically Erasable Read Only Memory. The Optech optical scanner stations in Maricopa that record 98% of the precinct vote also use Z80 processors and EEPROM memory packs.

The Princeton study showed that data on the memory pack could be altered by a device as small as a pack of cigarettes, or easier still a laptop or "palmtop" computer of almost any sort. Electronic alteration is simple because there is no encryption of the data in the pack – also known as an "electronic ballot box". See **YOUTUBE 07:12 minutes**: Sequoia Part 5: Manipulating Sequoia Results Cartridges could be easy in Maricopa County, AZ.

<http://www.youtube.com/watch?v=3bZvqTKOtlj>



*A standard EEPROM chip - something like this is inside the Sequoia memory pack...*

The Diebold optical scanners are roughly the same vintage and shared the same flaw. In the HBO documentary "Hacking Democracy", Black Box Voting and their consultant Harri Hursti went to Leon County FL and proved you could alter the contents of their memory cards, rigging them before election day so as to have negative votes for one candidate and positive votes for another *yet still show "no votes entered" if you check it on election morning by running a zero tape*. Such an electronically pre-stuffed ballot box will take votes from one

candidate and give them to the other, while printing an end-of-day tape at the close of polls that will look correct.

In a state such as Arizona where at least a small hand-count happens, one would think this would be too risk – *unless of course the county has made undetectable access to the paper ballots trivially easy...*  
The Diebold memory card physical format was very obscure and the BBV team had to search hard for an effective reader, buying a device online normally involved in measuring moisture in cornfields. The EEPROM technology used by Sequoia doesn't have that problem: while the connectors used for the memory pack are proprietary, the internal memory chip is a standard device. Given access to just one pack and a few minutes quality time with a screwdriver and continuity tester, it's possible to trace the pins from the standard EEPROM chip holder to the connections Sequoia creates. From there, making an adapter between a writer device for such chips and the Sequoia connector means about \$10 worth of Radio Shack parts and half an hour with a soldering iron. Build just one and it could hack as many cartridges as you'd like in rapid order.

As a final insult, while state law requires these memory packs to be brought in from the field by two people (one from each party), that clause is routinely ignored. While at a receiving station watching them come in, a number of pollworkers attempted to hand these off to us. The cartridges were in plastic bags with paper seals that can be peeled open if you do it slow enough, and can be re-sealed with no evidence of tampering.

#### 11) "TRANSPORTING THE MEMORY PACK" from Secretary of State Procedures manual page 143 Approved October 2007.

In precincts where transmittal is not done by modem:

- 5) place it in the container provided along with the tape,
- 6) for accessible voting units with a paper receipt, place the receipt in the container
- 7) seal the container,
- 8) the inspector and judges sign the seal, then
- 9) at least two designated election officials representing voters of different political parties shall deliver the container to the designated receiving site.

**NO SEALS, 1 PERSON DELIVERING.** Here is a video we shot that proves that the above procedure was not done: <http://blip.tv/file/1437202/>

#### 12) CENTRAL TABULATOR SOFTWARE AND SEQUOIA ISSUES IN GENERAL

Sequoia has broken a number of rules regarding voting system certification in general. Some of these are specific to the central tabulator (WinEDS) and ballot preparation software (BPS). Voting system software is supposed to be reviewed at the Federal level and then in AZ again (barely) at the Secretary of State's office. Sequoia has very deliberately avoided oversight on several key components.

##### HERE ARE THREE KEY POINTS WHERE SEQUOIA HAS VIOLATED THE LAW:

1) Sequoia uses Windows CE ("Compact Edition") on one component (the "HAAT", "Hybrid Activator, Accumulator & Transmitter") yet didn't declare Windows CE's customized code to the Federally qualified test labs. The National Institute of Science and Technology recently de-certified one of the three original labs (Systest) and in their letter stripping Systest of the ability to test voting systems, NIST says:

The Windows CE customizing files were not reported as being reviewed as non-COTS source files. [ed: "Commercial Off The Shelf" or COTS software doesn't need full test lab review where custom stuff does.] An open question exists of how to report these files but the presence and review of these Windows CE customizing files needs to be reported to identified [sic] that they were missed.

In other words, NIST is blaming the lab for not catching on that WinCE is heavily customized by design - this "mini version" of Windows is a "kit" Microsoft puts out that the hardware vendor needs to complete rather than a complete system. However, the rules say the vendor such as Sequoia has to **declare** what's custom and what's not...so the sin is on both the labs for stupidity (three labs blew it in this fashion) and on Sequoia for fraud.

See also NIST's letter at:

<http://www.eac.gov/extlnk/lnkframehead.htm?http%3A/vote.nist.gov/NVLAP/SysTest-102808.pdf>

...on page 18 (as Acrobat numbers pages) section 5.10.1.

2) For their next trick, Sequoia has claimed that BPS is passing "software" from that uncertified system (BPS) and pumping it into a certified system (WinEDS). After our February analysis of the Maricopa operation we received a public records response to our query for the Sequoia database (including BPS data) drafted by Sequoia's vice president of certification. That letter says that the BPS data being transferred into WinEDS contains "proprietary software". Even if you accept that BPS doesn't need certification, there's no possible way a court will support an uncertified program pumping software into a certified system. **Nobody** can be allowed to do that if the system is to retain any credibility whatsoever.

3) Sequoia claims BPS doesn't need cert under the 2002 Federal standards...and so far the EAC and AZ SecState's office has backed that concept. However, that flies in the face of the Federal definition of "voting system" as codified in HAVA:

**SEC. 301 42 USC 15481.(6)(b) VOTING SYSTEM DEFINED.**—In this section, the term "voting system" means—

- (1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—
  - (A) to define ballots;
  - (B) to cast and count votes;
  - (C) to report or display election results; and
  - (D) to maintain and produce any audit trail information;

**BPS "DEFINES BALLOTS"** as the Maricopa County elections office knows. Given Federal law in this area, and the AZ legal requirement to follow the Federal standards, it seems likely a court would say BPS needs certification – which it doesn't have.

We even have some reason to suspect why BPS wasn't submitted for certification: **it needs MS-Access present in order to run.** Microsoft Access is well known for it's ability to get people into election databases and let them make alterations without leaving the normal "audit" lot traces...it's basically a burglary tool for elections. **Even the worst of the test labs would have choked on having it present in the field, required to make BPS work.**

### 13) MARICOPA LACK OF DETAIL ACCOUNTING BY BALLOT TYPE

True auditing of an election involves tracking where each vote and block of votes came from by category. Each category of vote (mail-in, precinct optical scan, precinct touchscreen, provisional and more) has it's own set of risks as to how it could be subverted. Knowing what the totals are for each category by date allows identification of unusual "spikes" or variances between categories.

Arizona is among the majority of Western states in which it is easy to sign up as a mail-in voter. As with other such states, the rate of mail-in voting hovers near 50% or so. If a candidate wins big at the precincts but loses big in the mail-in vote, the possibility arises that one or the other was subverted in some fashion - the bigger the discrepancy, the more attention should be paid.

Maricopa has made such analysis difficult bordering on impossible by "blending" vote categories. We consider this a serious failing.

On election night at 8:03pm, the county published vote totals for the mail-in vote to date. This made perfect sense as those were the only ballots scanned and processed; they had printed the "who's winning and losing" report at the first legal moment they could (one hour post polls close).

From that moment forward, no additional "mail-in vote numbers" were published, even though well over 300,000 ballots were remaining to be scanned. All of those votes were piled into the precinct totals - as were provisional votes, mail-in votes dropped off a the precinct and the military absentee votes processed through the AZ Secretary of State's site.

**Jim March wrote:**

***“It’s as if all parts of your dinner were run through a blender before being poured onto your plate. The results are about as palatable but in the case of the Maricopa elections process, the result isn’t nausea: it’s an inability to track what’s going on and spot problems that may be related to security risks to one class of vote versus others”.***

Other AZ counties including Pima break their numbers out in much more detail. Maricopa’s process needs to be reviewed against that of other agencies in and out of Arizona.

#### **14) PUTTING THE PIECES TOGETHER IN MARICOPA: A BLUEPRINT FOR A HACK?**

All the pieces are present (and then some) to pull off the “immaculate hack” - alter both the paper and electronic records to match in a vote tampering attack that can never be detected.

- A. The paper records are vulnerable due to duplicate seals, poor quality ballot boxes (or bags) and storage in insecure locations. Altering the paper records for all ballots on a county-wide race might be possible if you just “shave” ten or so votes per precinct. Doing so for a race that doesn’t cover the whole county, such as one of the smaller city councils or any of the various board positions would be easier. Extra ballots are available through via one of the same printers Runbeck’s “Sentio” uses, or just deliberately overvoted a candidate position when the voter votes “incorrectly” for a certain candidate.
- B. You wouldn’t need to alter the central tabulator record at all. Best approach would be to hack the memory cartridge, print out a new results tape (unsigned same as the original) and re-feed that into the central tabulator.
- C. You can do anything you want to the mail-in votes at the central tabulator, because you know which batch numbers CAN be “audited”. You’d be taking a minor risk that the scanners might have malfunctioned on the “audit” batches and the counts might not come out right – but that’s OK, subverting the hand “audit” ahead of time by making sure the mail-in hand “audit” batch counts come out perfectly is child’s play: find out from the computers what votes are supposed to be in the “audit” batches, open the box either with the centerpunch stunt or your handy spare seals and make sure they’re right. When hand “audits” come out perfect, you can be sure nobody will dig deeper.

***IT WOULD BE ALMOST IMPOSSIBLE TO DESIGN A SYSTEM END-TO-END THAT WOULD FACILITATE FRAUD BETTER THAN WHAT WE’VE FOUND IN MARICOPA COUNTY.***

The day after the election when the parties were picking precincts and races to “audit”, we raised these concerns and asked the county to put extra seals of the “sticky” type at the four corners of the mail-in vote “audit” batches and to allow us to put additional seals on the 23 precinct’s ballot that were picked out of the 1,142 precincts. [This was met with angry refusal.](#) Link to audio excerpts of our complaints that morning are online at: <http://www.youtube.com/watch?v=9oAczDmbWww>

At every step, this department in general and Ms. Karen Osborne in particular displayed a lack of concern for real security while ensuring that “security theater” involving metal detectors, rules about “no cellphones, no laptops” and other such silliness was the rule.

While that was going on, she actively worked to make sure she could tamper with the vote at any time. A classic example involved the mail-in vote “audit” box seals. They were always ceremoniously taken out two at a time, each individually numbered (two seals to a box) – neglecting to mention they had an additional 19 seals of each number in the back room in case they needed to get into those boxes.

That was a bitter insult to all of the volunteers from the Republican, Democratic and Libertarian parties who put in long boring hours to make sure this process went smoothly and fairly. For our effort, we were treated to a meaningless show, a Potemkin Village of an election, barred from going anywhere else in the building or inspecting what goes on behind their closed doors and layers of secrecy.

Sadly, on top of everything else, on November 4<sup>th</sup>, 16 voters out of 100 that voted at a precinct in Maricopa County (Phoenix) had to vote a provisional or a conditional provisional ballot.

#### 15) SO WHAT'S THE CURE?

Last December 19<sup>th</sup> the headline in the Tucson Citizen read "**Pima County to spend up to \$10 million to improve ballot security**". That included the purchase of an entirely new voting system for about \$5 million.

Immediately after hearing this Jim March and I opposed this idea due to the fact we know there is nothing else out there at this time or for the next 2 to 4 years that's any better. We know that we're voting on a fatally flawed system and the only solution at this time is transparency, transparency and more transparency. As I've stated above, as bad as that Diebold system is, it's better than many other voting systems that exist at this time, it's better for all of us to work with the devil we know rather than the devil we don't. **So please help us get more transparency.**

#### BUT WHO WILL DELIVERER THAT TRANSPARENCY?

In Arizona we had to learn through litigation in Pima and Maricopa County that **NO ONE REPRESENTS THE PUBLIC** when it comes to verifying that elections are honest. We know this from our work and the deposition of Jan Brewer's State Election Director Joseph Kanefield:

**Testimony in a deposition of the Arizona Secretary of State's office under Rule 30 (b) (6)** designee was Joseph Kanefield, State Election Director, April 11, 2008. Stated on the record that his office doesn't have the authority to examine election databases, how could this be?

#### IMPORTANT EXCERPT OF DEPOSITION:

Q. *BY Attorney William 'Bill' RISNER: First, can we clearly establish that your office never has gone in and examined a database to see if there's been any fraud or manipulation?*

A. *Mr. Kanefield: Our office doesn't have the authority, under law, to do such an examination. Our -- the extent our office has oversights over a potential fraud investigation would be pursuant to the statute we discussed earlier, where a copy of the election software and database structure is filed with our office. And at that point, we would make that available to the Attorney General. **THAT'S ONE OF THE REASONS IT HAS TO BE KEPT CONFIDENTIAL**. So are we going in and are we examining county databases and computer programs? We don't have the authority to do that. I mean, the Secretary of State's authority is prescribed by law, AS SET FORTH IN THE CONSTITUTION, and she's been given oversight over a number of election-related activities, including logic and accuracy testing and other related issues. But when it comes to the administration of the elections at the county level, what you're talking about, if you're -- **IF YOU'RE ALLEGING THAT WE SHOULD HAVE BEEN DOING THIS AND HAVEN'T, THEN YOU'RE WRONG**. We just simply don't have the authority to do that. If we were provided that authority, then, of course, we would do that. But we think that the process works and that if those allegations are made, then those with authority -- including the County Attorney, Attorney General -- can undertake such review, as was done by the Attorney General at your request.*

Q. *BY MR. RISNER: Are you aware of any county in Arizona that has ever conducted a post-election examination of the database for evidence of fraud or manipulation?*

A. *MR. KANEFIELD: **I am not aware**, other than what's occurred in Pima County. But that doesn't mean it hasn't happened. It's just that I'm not aware.*

Q. *BY MR. RISNER: Okay. So the result, then, is that the Secretary of State, because it has no authority to, does not examine and has never examined an election database after an election in any county in Arizona; correct?*

A. *MR. KANEFIELD: **That is correct**.*

Youtube, 2 minutes, KOLD TV Tucson 4/21/08, "WHO CHECKS THE VOTE COUNTERS?" It is NOT the Secretary of State! Not the Attorney General! Not the County!: <http://ca.youtube.com/watch?v=fqleflQVkrk>

From the process of discovery in Pima Co. several important bodies of work have been produced that have within them the potential that could help with creating trustworthy elections.

**These elements are:**

1) We're making a documentary called "Fatally Flawed" A DVD/video which will:

- a) Review the nationwide implications of the precedent-setting Pima Co. court case that reaffirmed and established that the databases are Public Records to be available for public scrutiny.
  - b) William 'Bill' Risner Esq. will be laying out the facts to the RTA bond election and making a case to the public that election fraud is real, thus assisting us by whipping up public pressure to demand a proper criminal investigation.
  - c) From the examination of the databases comes the possibility to detect and verify databases manipulation. (Vote flipping and hacking) in other election.
  - d) Explain a number of ways the vote can be hacked or manipulated from inside the machines
    - 1) Company preprogrammed memory cards to influence the manner that votes are counted.
    - 2) Use of uncertified software.
    - 3) Physical manipulation thru Microsoft access of the databases.
- 2) We designed a special computer program to analyze the Diebold computer logs and databases of the central tabulations to see whether manipulation has occurred. Tampering at the memory cards may show up in this software depending on the type of manipulation. Automated reports on patterns of voting throughout an election cycle will be part of the program and will allow for fast "sanity checks" of an election cycle in time to file legal challenges. Currently a software program is in beta testing.
- 3) Maricopa Project - we have started a detailed examination of the Maricopa County election process along with the Sequoia gear it runs on. As you know now from above there are major flaws. A key concept that we believe will be valid in most states is "electronic voting must include effective electronic observation". When state observation laws rely on human eyeballs alone in this electronic age the ability to fully observe the process and results will never be thorough, and complete. This concept can be used to push for reforms WITHOUT a total legislative overhaul, by taking a functional approach to existing legislation.
- 4) **LEGISLATION TO GRAPHICLY SCAN THE VOTE.** Voting is a secret process, counting the vote is a public process. The idea that ballots can be graphically scanned and then distributed to any interested party could be the main breakthrough we need to ensure accurate elections. A systematic model is established in each county where a certain percentage of the ballots are photo scanned with graphic scanners and put on the Internet for public transparency and scrutiny, which can be checked against a physical audit. However, at present SoS Jan Brewer is blocking it with spurious legal arguments. Sen. Johnson prepared and sponsored legislation at least allowing the scanning of ballots in standard commercial graphic scanners ("white boxes") after they come out of the standard voting machines ("black boxes"). Given this opportunity Pima will jump at the opportunity and others will follow. Graphic scanners are far cheaper than changing from one unreliable set of "black boxes" to another (Diebold to Sequoia, etc.).

Simple this is how it would work. On election day, 10% of the precincts shall be randomly selected by drawing. That evening as the polls close, a special group of pre-selected pollworkers will travel to those precincts with a laptop computer and small scanner and at the close of polls will scan those paper ballots plus the various end-of-day reports, printouts and the like. Like the larger scanners used to process the mail-in and provisional votes, these smaller systems and scanners must not have optical character recognition ability and must write the output scans to write-once media. Copies of this media will be made available at the polling location to those interested, and made available later by the same means as the larger graphic scan collections on the internet, marked as to the precinct they came from and method of scanning.

The rest of the precinct paper vote, as it arrives at the jurisdiction's main election processing scanner, shall be scanned on the same large graphic scanners that process mail-in and provisional votes, handled in the same manner but identifiable as to precinct and scan type.

- 5) **EDUCATION, EDUCATION, EDUCATION** of election personnel, legislators, and grass roots people to put the pressure on their officials and become the auditors of a transparent system that assures every vote is counted accurately as intended. We at AUDIT-AZ and EDA work with all groups from the sincere Right and Left.

**AS TO ELECTION ASSISTANCE COMMISSION.**

The EAC, formed in 2002, to date still acts as if it were still a steering committee with no real power to enforce security standards. This model dominated and influenced by vendors who control the certification process, permits the establishment of voting systems like the one described in Maricopa County with no built in security that appears to be designed to allow wholesale vote tampering. When votes are counted by insecure systems in secret, the public interest that votes be counted accurately and transparently can be easily subverted, and we no longer have a democracy.

Too much is at stake. This needs to change! A democracy must be built on transparency and verification, not blind faith.

Elections are just too important.

I thank you for your consideration.

Respectfully yours,

John R. Brakey,

Co-founder of AUDIT-AZ (Americans United for Democracy, Integrity, and Transparency in Elections, Arizona) & Co-Coordinator Investigations for Election Defense Alliance [http://www.electiondefensealliance.org/about\\_john\\_brakey](http://www.electiondefensealliance.org/about_john_brakey)  
5947 S Placita Picacho El Diablo  
Tucson, AZ 85706  
520-578-5678  
Cell 520 551 5492