



**ELECTION
DEFENSE
ALLIANCE**



Voting Counts

...when Your Vote is Counted.

EDA & AUDIT-AZ's MISSION: 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.

**ELECTION DEFENSE ALLIANCE & AMERICANS UNITED FOR DEMOCRACY, INTEGRITY,
AND TRANSPARENCY IN ELECTIONS**

THE ARIZONA ELECTION TRANSPARENCY PROJECT

JOHN BRAKEY AND JIM MARCH
5947 S. PLACITA PICACHO EL DIABLO
TUCSON, AZ 85706
AUDITAZ@COX.NET JIM.MARCH@GMAIL.COM
JOHN 520-250-2360 / JIM 916-370-0347

Thursday, June 12, 2008

Digesting Brewer's Brew: A Close Analysis of A Written Declaration Of War Against Election Transparency

By Jim March and John Brakey

Introduction:

On 6/6/08 Arizona Secretary of State (SOS) Jan Brewer wrote an 11 page letter outlining objections to the election integrity process in Pima County.

Beginning in 2004 Pima County citizen election integrity advocates working with and within the Pima Democratic Party found that the county government and to a limited extent the election department were able to cooperate to improve the level of security and transparency in the Pima County elections process. These changes included:

- * Rebuilding the central vote tally room so that all wiring was visible, eliminating the chance that the election was being “back door controlled” by an extra, uncertified and unseen system or network.
- * Additional computer monitors show observers what is happening on the central tabulator computers.
- * The central tabulator computers were put in a lockable cabinet the size of a phone booth. This cabinet could be locked and by policy tamper-sealed when not in use.
- * Modem communications allowing the Diebold touchscreen voting systems were disabled as that data channel opened an obvious “hacking channel” from the outside world¹. This policy was later extended to the Diebold optical scan stations².

¹The Diebold touchscreens communicate with the central tabulator via a Microsoft product called “RAS” for “Remote Access Server”. MS-RAS is no longer supported and has horrific security flaws.

²While the optical scan stations don't use MS-RAS, they communicate on a similar if more primitive protocol designed in the mid-1990s by the companies Diebold bought. It's more obscure, but many ex-Diebold people plus current or former elections staffers with a hacking bent would know how to exploit it. Like the MS-RAS modem link, it's an open path to hacking into the central machines that run elections.

These and other improvements improved election integrity and transparency in Pima County. However, cordial relations suffered after county officials delayed access to public records in late 2006, and then denied access to the raw election files post-election in early 2007. This denial led the Pima Democratic Party to file suit and battle a year-long hard-fought litigation. When the dust cleared:

* The Pima Democratic Party obtained full access to every raw election data file going back to 1998, and all records in future elections once each election officially ended are to be given if requested to all parties on the ballot.

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

Q. BY MR. 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.

Must see TV! Two minutes says it all. 4/21/08 KOLD TV Tucson: facts learned in the Pima Co Democratic Party's election integrity lawsuit - from deposition of Jan Brewer's State Election Director Joseph Kanefield: "WHO CHECKS THE VOTE COUNTERS?" NOT the Secretary of State! Not the Attorney General! Not the County! By Bud Foster, 2 minutes long:
<http://ca.youtube.com/watch?v=fqlefiQVkrk>

* The county's own expert witnesses had to admit that the Diebold voting system products are of low quality with substandard security. They also noted that the rest of the voting systems certified for use by both the Federal and Arizona state approval processes suffer from similar or worse issues; the Pima Democrats and their allies agree.

Faced with the new information from the lawsuit, Pima County's first reaction was to dump the FATALLY FLAWED Diebold system. Last December 19th 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.

As veterans of both sides of the litigation reminded the county's leaders, the other systems are no better. Therefore, the solution is transparency, transparency and more transparency. The Pima Democrats and their allies suggested an alternative: keep the Diebold equipment but apply a "security patch" involving scanning the paper ballots already processed in the Diebold systems in separate "graphic scanners" that take snapshots of each ballots. These could be distributed on the CD or DVD to anyone interested and even put up on the Internet, allowing "recounts" by volunteers at home.

The fix we're taking about is under \$150,000 vs. \$5 million. Fact is the Diebold System is better than many other voting systems that exist at this time. Right now, we think it's better for all of us to work with the devil we know rather than the devil we don't.

Pima County took important action to turn off the optical scan modems to disable would-be hacking attempts, and have recommended taking out the touchscreens from now on since these machines are faulty and have been largely rejected by disabled voters.

AZ Secretary of State Jan Brewer, an enthusiastic promoter of touchscreen voting, promptly went ballistic. Let's examine her latest missive of 6/6/08.

June 5, 2008

C.H. Huckelberry, County Administrator
Pima County Administrator's Office
130 W. Congress
Tucson, Arizona 85701-1317

Dear Mr. Huckelberry:

Thank you for sharing with my office a copy of your Final Report Regarding County Modifications to Election Procedures to Enhance Security and Reliability of Election Results. My staff and I have carefully reviewed the proposal and I would like to share my thoughts.

Be assured, I have made it my top priority over the past five years to ensure that all elections conducted by our county election officials are run in a fair, orderly, accurate, secure and, perhaps most importantly, uniform manner. I have conducted an extensive review and examination of our election systems through the Brewer Voting Action Plan, successfully promoted legislation to provide additional layers of election security, and strengthened the security procedures set forth in the Secretary of State's Election Procedures Manual (Procedures Manual) followed by all of our county election officers.

If Jan Brewer's highest priority was security and reliability of elections she wouldn't have exposed herself to conflict of interest criticism by accepting the co-chair position of the Bush reelection campaign just as Ohio's SOS [Ken Blackwell in 2004](#) and SOS [Katherine Harris of Florida in 2000](#).

As to the "[Brewer Voting Action Plan](#)": One should go to these sections and read her own report. SOS Brewer wants to disregard our concerns even though, as we point out they are in her own report from May 3, 2005.

Excerpt of from [Brewer Voting Action Plan](#) published 05/03/05 APPENDIX - GARTNER ASSESSMENT OF ELECTION SYSTEMS REPORT – Index: you can see that Brewer’s own documents clearly warn of many of the same issues that have cropped up in Pima County.

3.0 QUESTIONS REGARDING CURRENT DIEBOLD ELECTION SYSTEMS	20
3.1 DO CURRENT DIEBOLD DRE ELECTION PRODUCTS HAVE SECURITY FLAWS?-----	20
3.1.1 <i>Description</i> -----	20
3.1.2 <i>Analysis</i> -----	20
3.1.3 <i>Recommendations</i> -----	25
3.2 ARE DIEBOLD PRODUCTS VULNERABLE TO INTERNET ATTACKS? -----	26
3.2.1 <i>Description</i> -----	26
3.2.2 <i>Analysis</i> -----	26
3.2.3 <i>Recommendations</i> -----	27
3.3 DOES DIEBOLD HAVE A QUALITY SOFTWARE DEVELOPMENT METHODOLOGY?-----	27
3.3.1 <i>Description</i> -----	27
3.3.2 <i>Analysis</i> -----	27
3.3.3 <i>Recommendations</i> -----	28
3.4 DO DIEBOLD PRODUCTS HAVE ADEQUATE CONFIGURATION MANAGEMENT? -----	28
3.4.1 <i>Description</i> -----	28
3.4.2 <i>Analysis</i> -----	28
3.4.3 <i>Recommendations</i> -----	28
3.5 DO DIEBOLD PRODUCTS HAVE ADEQUATE PASSWORD MANAGEMENT? -----	29
3.5.1 <i>Description</i> -----	29
3.5.2 <i>Analysis</i> -----	29
3.5.3 <i>Recommendations</i> -----	30
3.6 DO DIEBOLD PRODUCTS HAVE ADEQUATE ACCESS MANAGEMENT? -----	30
3.6.1 <i>Description</i> -----	30
3.6.2 <i>Analysis</i> -----	31
3.6.3 <i>Recommendations</i> -----	31
3.7 DO DIEBOLD PRODUCTS HAVE ADEQUATE AUTHENTICATION OF ELECTION REPORTING? -----	31
3.7.1 <i>Description</i> -----	31
3.7.2 <i>Analysis</i> -----	32
3.7.3 <i>Recommendations</i> -----	32
3.8 CAN SMART CARD FRAUD OCCUR WITH DIEBOLD PRODUCTS? -----	33
3.8.1 <i>Description</i> -----	33
3.8.2 <i>Analysis</i> -----	33
3.8.3 <i>Recommendations</i> -----	34
3.9 DOES DIEBOLD HAVE ADEQUATE INTERNAL SECURITY? -----	34
3.9.1 <i>Description</i> -----	34
3.9.2 <i>Analysis</i> -----	34
3.9.3 <i>Recommendations</i> -----	34
3.10 DID DIEBOLD DISREGARD STATE-CERTIFIED CONFIGURATIONS? -----	34
3.10.1 <i>Description</i> -----	34
3.10.2 <i>Analysis</i> -----	35
3.10.3 <i>Recommendations</i> -----	35
3.11 IS DIEBOLD AN OBJECTIVE ELECTION PARTNER?-----	36
3.11.1 <i>Description</i> -----	36
3.11.2 <i>Analysis</i> -----	36
3.11.3 <i>Recommendations</i> -----	36
3.12 RECENT DIEBOLD ACTIONS IN RESPONSE TO CRITICS -----	37
3.12.1 <i>Some Perspective</i> -----	37
3.12.2 <i>In Defense of Diebold Election Systems</i> -----	37
3.12.3 <i>Response to Ohio Compuware Study</i> -----	37
3.12.4 <i>Response to the RABA Study</i> -----	38
3.12.5 <i>Diebold Announces Restructuring of Compliance and Certification Processes</i> -----	39
3.12.6 <i>Future of Diebold As Election Vendor</i> -----	40
http://www.azsos.gov/election/Brewer_Voting_Action_Plan/Brewer_Voting_Action_Plan_Final_05_03_05.pdf	

Since the release of Brewer’s Voting Action plan, we know more about the dangers of electronic voting. We conclude that after California SOS Debra Bowen released the results of a top-to-bottom review

³coordinated by computer scientists from top universities in California and the nation, the security of electronic voting has proven to be worse than we originally thought.

In 2006 John Brakey and Jim March were commissioned to travel around the state examining voting systems in advance of the general election. We evaluated how Brewer's "Voting Action Plan" and physical security provided by counties worked to protect election security and reliability. We spent over a week on the road, in many cases examining counties immediately following the pre-election logic and accuracy ("L&A") test run by staffers from Jan Brewer's agency.

We covered almost half the state; in all cases we were credentialed observers appointed by a county party chair.

We have personal reason to distrust the professionalism of Brewer's elections division staff and procedures. We saw all sorts of violations of procedures, certification principles and transparency. In one county we saw visible cross-wiring into the Internet, in another uncertified copies of MS-Access, all on systems that Brewer's people had allegedly "tested". In one case the only observation we could do of the central tabulator room was of the outside of a closed door on a windowless room; we complained to Brewer's people on-site about this observation law violation and they ignored us. We have documented our findings in written reports and photos.

SOS Brewer's letter to County Administrator Chuck Huckleberry undermines the County's laudable steps to establish better physical security:

Although some of your recommendations make sense, most are problematic, unnecessary and/or unjustifiable, and nearly all establish a protocol for Pima County that is vastly different from every other county.

***Our View:** Perhaps Brewer is thinking that since these security improvements don't come out of her office, they might make her look bad as this is her job...*

According to ARS 16-445 during a suit or investigation the SOS office is to hold the backups and provide them to the Attorney General office. Brewer's office did neither.

SOS Brewer tries to shift blame:

Before I begin, I must take issue with your implication that my office lost the RTA election tape that was filed by Pima County in accordance with A.R.S. § 16-445. This is simply false. My office testified that this tape was sent back to Pima County via U.S. Certified Mail on November 27, 2006, along with hundreds of other programs that were returned to the other counties and local jurisdictions.

It is a strange coincidence indeed that the only program reported lost was your RTA election program, which also happened to be at the center of some very serious allegations involving your election officials. I resent your attempt to blame my office for the convenient loss of this program by your staff. To reiterate, all other jurisdictions were mailed, and received, their programs and there is no evidence to suggest my office lost your program.

***Our View:** She omits the part about her office mailing the tape to the wrong department (Recorder's office) when it should have gone to the Election Department, which has allowed them a fig leaf of "accidental loss" excuse. Also, while a criminal investigation was going on by the Attorney General on the RTA race she never informs the Attorney General office that she has copies of the databases.*

³California Secretary of State Top to Bottom Review: http://www.sos.ca.gov/elections/elections_vsr.htm

BREWER'S LETTER OVERLOOKS FLAWS, MAKES EXAGGERATED CLAIMS

ELECTION SECURITY UNDER THE BREWER ADMINISTRATION

You note how anxious you are to learn about my proposals for reform. Thus, allow me to summarize the extensive voting security efforts that have already been implemented during the course of my administration with important security features being added for each of the past five years. This may help you better understand the extent to which I have taken it upon myself to bolster the security and integrity of our elections in Arizona.

It bears repeating that from an election security point of view, Arizona's laws and procedures establish a rigorous end-to-end approach that is among the tightest and most secure in the nation. These statutory and procedural security, educational, and accountability requirements include:

- Rigorously testing and certifying voting equipment at the federal and state levels to uniform and national standards set forth by the Election Assistance Commission as well as Arizona statutory requirements.

Arizona law places a limit on Brewer's powers: The Secretary of State can only certify voting systems that have been Federally certified first via a system of testing labs that have access to (and are supposed to review) the source code, and a Federal agency (Election Assistance Commission or EAC) to oversee the labs.

In at least two cases Brewer has approved systems that haven't been properly certified. Large sections of the software in the Diebold touchscreen machines (starting with the highly customized operating system) haven't been checked out by anybody, while Sequoia shipped a whole module that had never been certified - "BPS" creates the electronic and paper ballots, and then pumps large volumes of data into the certified system⁴.

Please understand that "certification" really means "somebody outside of the vendor has checked the code out" - an obvious barrier to fraud. It's not very effective, but at least it's something. Two vendors in AZ dominating the counting of our vote to both dodge it by routing key software components past the test process - that should scare the hell out of any one who wants to make sure his or her vote gets counted.

Brewer's office has done little more than bring systems into the state and "kick the tires" - they run a Logic and Accuracy test and a modest functionality test for a couple of days. They do NO "red team" type security analysis⁵ and no source code review. There is nothing "stringent" whatsoever about the AZ state process.

Our View: *What Brewer's staff does is a "kick the tires" test and run a "Logic and Accuracy" test.*

- Testing and inspecting all equipment after routine maintenance and after certified upgrades to firmware, software and hardware have been installed.

Our View: *Worthless if it's as sketchy as everything else we've seen...*

⁴ Sequoia is now on record as saying the BPS data files cannot be released under public records laws because they contain Sequoia's trade secret "software". This means that "software" of unknown type and size is being pumped into a certified voting system from an uncertified source.

⁵ A "red team attack" means that qualified security professionals take a complete voting system and acting as both voters and elections staff in separate scenarios attempt to subvert a test election. When this was done in California, every voting system reviewed failed miserably.

- Logic and accuracy testing before and after each election to ascertain that the equipment and programs correctly count the votes cast.

Our View: L&A tests provide false security.

Let's talk about L&A tests and what Brewer does not do.

The first issue is that it's usually possible to tell in advance, if you're the programmer controlling a machine, whether or not the test election being performed is a test or the real election. Some voting systems actually have a "test mode" which gives the game away completely, in others you can tell either by the date or by the predictable pattern of test ballots or both. However you do it, if you're the programmer you have the ability to have the machine behave honestly during the test and otherwise during the actual election. No meaningful steps to eliminate this possibility has been required at the Federal level or implemented at most state or local levels.

The second method of subverting the L&A process is to tweak the database following the L&A to make it perform differently than it did in the test. Post-election analysis of the data files for an election should be able to compare the L&A test state with the actual election state of the election setup. It is precisely this class of oversight that Brewer is actively seeking to block.

- Preparing and examining each machine before it is sent to a polling place.

Brewer makes it sound like they do the L&A test process. What her staff does in the field is run an L&A test just before the election on several machines in each county. However it's what they don't do that has us concerned: they don't check for illegal software, inspect the facility for security, or follow their own procedures manual. See previous comments. There's no adult supervision over the counties.

- Requiring equipment and ballots to be physically secured at all times.

This just isn't true.

All counties that we are aware of, including Maricopa, have been doing voting machine "sleepovers", sending them out with pollworkers up to days prior to the election or leaving them unattended at polling places. Brewer's office had no qualms with this controversial practice. This is one of the points now cleaned up in Pima: at the request of citizens and party officials, sleepovers don't happen here.

In this and many other areas, Pima's standard of conduct is now far in advance of Brewer's standards.

- Prohibiting access to ballots and equipment without prior authorization.

Our View: Put another way: make sure nobody outside of the "election insider family" knows anything about the voting systems pre-election or post.

To understand how disgusting this is, refer to California Election Code 15004:

15004. (a) Each qualified political party may employ, and may have present at the central counting place or places, not more than two representatives to check and review the preparation and operation of the tabulating devices, their programming and testing, and have the representatives in attendance at any or all phases of the election.

This is a transparency measure with teeth. If we're going to have electronic voting, then we'd best have

expert computer “geeks” scope out the systems who aren't beholden to the election industry.

When we proposed this here in Arizona, we were told in no uncertain terms that the county elections officials and Brewer would be dead set against it. And given their stonewalling on other legislation, we took that as gospel.

Nonetheless, the basic idea that only election insiders know anything about what we vote on is a direct statement that county elections officials have a practical right to hack votes⁶. To any semi-qualified or better computer tech, the implications of a “total obscurity” policy are obvious.

- **Maintaining an inventory of all election media (e.g. memory cards).**

***Our View:** Maintained by insiders, who per Brewer have a practical right to cheat. Color us unimpressed.*

- **Requiring all election media to be secured at all times.**

We've personally seen examples otherwise. The worst involved Santa Cruz County (AZ) where the central tabulator room doubled as a hallway between two departments, contained computing gear beyond what was used in elections (so it was accessed by multiple departments and had Diebold memory cards stacked in heaps held together by rubber bands.

- **Requiring computer programs that run elections to be filed with the Secretary of State and held in escrow before the election.**

Just not true. We keep finding uncertified software all over allegedly “certified” systems. Even setting aside a disagreement about (the Windows CE customized operating system in the Diebold touchscreens or the Sequoia BPS module), we've found Microsoft Access in Maricopa after the systems were allegedly “reviewed” by Brewer's people. There has been NO significant review of any system's configuration out of Brewer's office.

- **Establishing a strict chain of custody procedure (i.e. secure storage, authorized access, two person transportation requirement) to assure that all equipment and software is accounted for at all times.**

***Our View:** “Sleepovers” expressly violate the assertion of a strict chain of custody.*

- **Requiring all election management software and equipment to stand alone and not be attached to any other computer or the internet.**

***Our View:** Yes, good idea if implemented.*

In Maricopa County, wiring between the voting system components in the '08 Presidential primaries ran up through the ceiling panels where it could be cross-connected to anything. As an official observer in that election cycle, Jim March asked Maricopa staff to “ping google”⁷ and was flat refused. Yet again, election officials maintain their practical right to cheat and when they do, there is zero recourse through Brewer's office. See Maricopa report:

⁶ A “practical right” is anything that you can do with zero chance of getting caught. Shut down all law enforcement and private oversight in a given area or legal circumstance and you create a “right” to commit crimes in that area. That's what Brewer is doing.

⁷ The “ping” command (ping www.google.com) has a computer briefly try to make contact with another machine (in this case google) and report back the speed to and from that system. It is a quick diagnostics tool that needs about 10 seconds to run. There was no excuse offered or possible for this refusal.

<http://www.bbvdocs.org/sequoia/Maricopa-County-Elections-Report.pdf> *Pay special attention to Appendix A in the full report:*

- Requiring election equipment firmware and software hash codes be verified against the National Institute of Science and Technology database before each election to assure the integrity of the software used at every election.

This assumes that the code is any good to start with, has been properly reviewed, ALL code has been submitted, etc. Brewer's office doesn't do such checking...

- Requiring that the installation and modification of any election management system software or computer programming used for county election administration be observed by a non-election employee designated by the Board of Supervisors.

***Our View:** Wait, what? We're going to have county employees, not independent computer experts check out the conduct of county employees? Sounds independent to us...not.*

- Prohibiting the use of wireless communications.

This is one thing that party techs and/or activists can check, via a laptop running WiFi Radar or similar.

BREWER'S CHARGES AGAINST PIMA ELECTION SECURITY REJECT TRANSPARENCY AND INDEPENDENT OVERSIGHT

The evidence shows that SOS Jan Brewer has failed to implement a plan for secure voting in Arizona. Her letter emphasizes her authority as SOS to define voting procedures and reiterates steps recommended to her by consultants. Her thinking is based on a flawed concept that trust in professional election officials and secret vote counting ensures security. She lacks a comprehensive understanding that accurate vote counting cannot be ensured at all without transparency and independent public oversight. Therefore the points she makes in her letter are based on a lack of realistic assessment of how some of her procedures actually work, whether they are implemented completely and honestly and whether following any of these procedures automatically yields fair elections and accurate vote counts.

Brewer's letter lists recounts mandated by law before Brewer took office as a recommended security measure. Even though Arizonans vote a paper ballot it is not likely that ballot will ever be recounted because to qualify for a recount the margin must be 1/10 of 1%. What Brewer fails to disclose is that Arizona's recount law, the most restrictive of any state in the country, works to make recounts rare because few elections fall within that thin a margin. Florida, also optical-scan paper ballot state unfairly restricts recounts to a 1/4 of 1% margin between candidates. A full and fair recount would provide a check on election results if candidates could actually ask for a recount and be charged a reasonable amount.

The only "transparency rule" in this ENTIRE list of Brewer's bullet points is the installation of live surveillance cameras installed in vote counting rooms uploaded to the SOS web site, but this measure is of limited usefulness. We have cameras at all thanks to our friend Republican State Sen Jack Harper.

WHAT'S MISSING? TRANSPARENCY!

What's missing from the whole list of "Brewer's security improvements" is any thought towards having the counties **prove to political parties and/or citizens that the vote was counted accurately**. Brewer does not recommend, authorize or carry out independent tech inspections. Brewer sets no barriers

stalling or denying public records access⁸.

In short, what we find throughout Brewer's "security thinking" is no concept whatsoever that county election official must prove to the parties and citizens that elections are conducted fairly. Without that thinking present, we find Maricopa County threatening to arrest observers who dare bring binoculars into the room to better observe parts of the process the county wants hidden. We see the refusal to "ping google", just about the simplest test imaginable and the most harmless.

We see an attitude across most counties, spurred on by Brewer, against transparency. An election conducted in secret is not a democratic process. The basic foundations of Brewer's ideas of election security lack the very concepts of transparency and independent oversight. This trend screams out across her whole letter as an underlying theme and from as seen in paragraph needs no further comment.

SOS BREWER REPRIMANDS PIMA COUNTY

PIMA COUNTY RECOMMENDATIONS

With regard to your April 3, 2008 report to the Pima County Board of Supervisors, I am at a loss as to why Pima County would argue in court against the release of election databases and then turn around and immediately release more databases than ordered by the court. It is no surprise that the court reversed itself in the post-judgment proceedings and ordered the release of this information given the actions by the Board.

The court's clear finding in its earlier ruling was that the release of additional databases may increase the risk of a security breach in a future election. Thus, all of your security recommendations mean nothing if the Pima County Board of Supervisors chooses to ignore the advice of its counsel and its own election experts. Quite simply, the Board's unilateral actions have placed all of our elections in jeopardy. I hope that the Board will make future decisions involving election security based on sound reason and judgment and not as a result of pressure from a handful of partisan rabble-rousers.

***Our View:** And here Brewer (or whoever wrote this for her) shows themselves to be technically CLUELESS.*

Background:

In his initial decision Judge Miller left the door open for us to get the rest of the databases. Basically he was being cautious until he heard further argument.

An election cycle can be said to run from the pre-election L&A test to the post-election L&A. In other words, once an election database is designed, complete with ballot layouts, candidate info, precinct data and the like, it is tested with fake data to make sure it can run the election. That's the main goal of the pre-election L&A. When that's done, the test votes are cleared out but the rest of the database is legally "frozen" - election officials aren't allowed to alter it. They can of course feed votes into it through the process, they can print election results after polls close and of course the audit log will increment as all these things happen.

But the basic "structure" of the election must, by law and Brewer's manual, remain frozen.

The easy way to hack an election is to tweak with these legal frozen elements.

⁸ After the 2006 general election Pima County stalled on public records access for over a month. Once we obtained audit logs, Windows event logs and the like, it appeared likely somebody had stolen the "who's winning and losing data" from the pre-election scanning of mail-in votes. When we asked to review the videotapes of the room, "so sorry, the video has auto-deleted itself due to a rotation cycle". Access to public records is a civil right and a right delayed is a right denied.

If you flip candidate IDs, you exchange their votes between them. Illegal as hell but also dead simple to accomplish as well as many others ways the system could be gamed and hacked.

It is also these frozen “structural” elements of the election that are the aspects of the database Pima County and Brewer wanted to keep confidential. It is these frozen elements that Diebold briefly tried to assert trade secrets on before giving that up, and that Sequoia is still holding firm on in Maricopa.

Throughout an election cycle, it's normal for elections managers to save backup copies as they go – starting with the initial L&A test and proceeding through each day's work or block of major activity. So we end up with a series of “snapshots” of the data from one end of the election to the final.

They are all SUPPOSED to contain the same “confidential” info (as Brewer sees it and Pima County argued). So if you release just one and not the rest as Judge Miller mistakenly, originally ordered, you're letting the cat out of the bag in terms of the “secret stuff” yet NOT allowing actual oversight by checking to make sure the “secret stuff” remains frozen per law. That thinking is behind Brewer’s sharp attack on the Pima County Board of Supervisors’ decision not to appeal Judge Miller’s ruling. Brewer just has it wrong.

The Jan. 8th 2008 Pima Board of Supes meeting was hardly a partisan affair; it was well attended and supported by other parties including GOP Congressional candidate Randy Graf and other Republicans. Libertarian Jim March asked the Board to ask their own expert⁹ one simple technical question:

“Is there any possible difference in election security between releasing one data file per election, and the whole suite of data files for a given election?”

The answer Pima County IT Manager John Moffat gave was “NO”. Given that, the order by the board to release all data files for the elections covered was a matter of course. Worse for them, this incident showed that Pima's defense in court had managed to bamboozle the judge to issue a ruling that could not be supported by the technical facts on the ground. Once he obtained the transcript of this discussion at the board meeting, his reversal of this point was assured and he lost all confidence in the technical grounding of all the defenses' claims¹⁰.

1. Impact on Other Counties

Your suggestion that the new election reforms proposed by Pima County could be enacted as options for the other counties is simply not workable. Although you claim that you do not wish to impose your election security standards on every other county, what you propose would in effect create a standard by which all other counties would be judged, without ever having sought input from those counties. It is simply bad policy for one county to push its agenda (which appears to be largely driven by local politics and not on reasoned analysis) on every other county.

***Our View:** Brewer implies that Pima County’s reforms may be desirable, but argues that the reforms would be unworkable in other counties. We have shown that basic computer security on the voting machines in other counties is indeed deficient when compared to Pima. But whose fault is that?¹¹, and should that be a reason to cripple election transparency anywhere in the state, let alone Pima?*

⁹ Mr. John Moffatt, basically a computer systems troubleshooter for Pima County who was assigned to tighten security at the elections office.

¹⁰ Jim March speculates that after the initial ruling ordering “one data file per election”, Mr. Moffatt likely realized the judge had erred. Either he didn't communicate this to his sides' attorneys or they blew him off; in any case the defense would have been better off pointing this out right away and preserving technical credibility; as it was, once the truth came out at the board and that got back to the judge, everything else was a foregone conclusion when reviewed by the court.

¹¹ Hint: initials are “JKB”...

From the court trial here is the testimony of Gila County Election Director Dixie Munday. Pay special attention to the cross by attorney Bill Risner:

<http://video.google.com/videoplay?docid=5020955874510327864>

Ms. Munday is the first witness called by Pima County. They sought to illustrate that release of the database could harm counties with less security. They wound up eliciting a security horror story that undermined their own position. Gila County has their Diebold/GEMS database prepared by a contractor. It is not checked by any independent or internal expert. The voting process is completely open to fraud occurring anywhere upstream in the production process, either by vendors, the contractor, or a third party able to penetrate the security of any upstream party. It is a truly ghastly situation. The Director relies solely on logic and accuracy tests that can be easily faked by anyone with access to the MDB database prior to those tests. Dixie Mundy has been the Gila County Director of Elections for 16 years. She is a member of the "Election Officials of Arizona" and one of twelve counties in Arizona that uses Diebold voting systems.

The database contains parameters of elections, ballot layouts and the ability to generate reports. A consultant lays out the ballot for Gila County. The consultant uses the previous setup in the database and modifies it for the new election. Mundy is unaware of any security problems in GEMS. She believes that if there were problems, the Secretary of State would have notified her. Her statement that she had no such warning from Brewer's office shocked the court which had heard evidence of fatal flaws.

SOS REPEATS MYTH THAT TOUCHSCREEN VOTING MACHINES HELPS DISABLED VOTERS:

2. Discontinuing the Use of Touchscreen Voting Devices

I strongly disagree with your proposal to discontinue the use of touch screen voting devices. This would violate federal and state law and would unnecessarily disenfranchise Pima County voters with disabilities. These machines must be used in every polling place to accommodate voters with disabilities.

The fact that so few voters use these machines establishes either (1) that the procedures are working properly as non-disabled voters are voting on the optical scan equipment and leaving this equipment available for voters with disabilities or (2) that Pima County has failed in its responsibility to reach out to the disabled community and educate these voters about the availability of these voting machines. Based on a recent complaint I received from a disability rights group regarding Pima County's failure to accommodate voters with disabilities, I have to assume it's the latter.

The abuse of the disabled community to provide excuses to push junk voting systems has a long and sordid history. It really goes back to an old stunt Diebold pulled before they bought Global Election Systems in 2002: they paid the National Federation of the Blind \$1mil which in turn financed "disability access" lawsuits against banks that didn't use Diebold ATMs. When Diebold got involved in voting (and the lobbying for the Federal Help America Vote Act) in 2002, this partnership with NFB continued and set the tone for a lot of tragedy since. http://www.wheresthepaper.org/Diebold_NFB.pdf

Brewer's missive here is simply the latest incarnation of the concept – Diebold and the rest have taught her well. Private voting for the disabled is important, but not at the cost of basic computer security or violations of the certification rules.

Brewer also brushes aside the facts to insist upon touchscreen voting. Touchscreen voting machines do not accommodate the disabled. See [the California Accessibility Review](#).¹² Researchers found that none

¹² Accessibility Review Report for California Top-to-Bottom Voting Systems Review

of the touchscreen electronic voting solutions fulfilled provisions in the current law and none were usable in test voting by persons with a range of disabilities and language needs. As a result, most blind and disabled voters in Arizona have refused to use them.

The "Executive Summary" of the California Accessibility Review says it all:

“Three voting systems, the Diebold AccuVote TSx, Hart eSlate and Sequoia Edge I and II, were evaluated for usability and accessibility for voters with disabilities and voters with alternate language needs, using both heuristic and user testing techniques. Although each of the tested voting systems included some accessibility accommodations, none met the accessibility requirements of current law and none performed satisfactorily in test voting by persons with a range of disabilities and alternate language needs. In some cases the accessibility or usability deficits could be partially or wholly mitigated. Some of these mitigations would not require new federal and state certification testing.”

Notice that the researchers say, "none met the accessibility requirements of current law." That's federal *and* state law. The machines have been sold for years --- and, in fact, the use of DRE machines as a whole has been jammed down America's polling places --- on the basis that they meet federal HAVA mandates for an accessible means of voting in every polling place. And yet, the California analysts found, they are not accessible at all...

Who decided these machines met the standards for accessibility in the first place? That would be the Independent Test Authorities (ITAs), which originally certified that the machines met the federal "Voluntary Voting System Standards." The ITAs are a small consortium of test labs, chosen and paid for by the voting machine vendors themselves. Next, the National Association of State Elections Directors (NASSED) Technical Panel reviewed the ITA tests and gave their stamp of approval by pronouncing these systems "federally qualified." Yet California's report shows without a doubt that the machines do **NOT** meet the standards and that they should *never* have been qualified for use by NASSED.



They didn't even get the positioning for wheelchair users correct.

“DREs: The VVSG requires a minimum of 30 inches of toe and knee clearance. No machine provided that clearance. This deficit posed a problem to almost every wheelchair-using voter in this study.” [Note that the use of the DREs presented an accessibility obstacle for fully-sighted wheelchair users with full manual dexterity, who do not require assistance to mark a paper ballot.]

Interference with Wheelchair Controls and Armrests

“DREs: eSlate and Diebold both interfered with the wheelchair controls.

BREWER'S EQUIPMENT REFRESH POLICY ASSUMES NEWER IS BETTER. WHO BENEFITS?

Absent from your report is your earlier recommendation to replace the voting equipment used in Pima County because it is nearly 12 years old. I once again agree with this proposal as it is consistent with my Equipment Refresh Policy set forth in the Election Procedures Manual. This policy recommends that the counties plan and budget to have all voting system hardware replaced at a minimum of every 10 years.

Our View: If all existing choices that Brewer allows Pima to purchase are ghastly, better to sit on their pennies and wait until decent gear is allowed onto the market.

BREWER DISAVOWS RESPONSIBILITY, TOWS DIEBOLD LINE

Lastly, I'm appalled at your suggestion that Pima County had no choice but to acquire the Premier touchscreen voting devices because of my decision to award the accessible voting contract to Premier. As you note on page 2 of your report, it was Pima County's decision alone in 1996 to purchase the optical scan equipment still in use today. In other words, I had no choice but to procure the Premier (then Diebold) equipment because of Pima County's decision to purchase Premier equipment in 1996. The Premier touchscreen equipment was the only equipment certified on the federal and state levels to work with Pima County's overall system. Thus, there were no other compatible accessible voting devices available. It is misleading and false to perpetuate to the public that you were not totally and completely responsible for purchasing Diebold equipment for Pima County voters to use. Your County's decision alone, forced the issue.

At the time the Diebold touchscreen systems were being considered, a competing plan involving the "Automark" device was proposed. The Automark is an odd duck: it acts like a touchscreen for the disabled community, but it produces a paper ballot that gets processed along with all the other paper ballots. As a "ballot marking device" the security issues are at least somewhat better: the Automark does not pump electronic data into the central tabulators. A viable plan to use these to mark Diebold paper was proposed, but Brewer and supposedly Diebold objected. Brewer stated this was purely because they objected to their paper being marked with somebody else's device. We provided names to Brewer of election directors in other states that were using the Diebold/Automark combination. *At this time the AutoMark is marketed by Diebold.*

SOS BREWER'S OPINION UPHOLDS ARIZONA ELECTION LAW

3. Modifying the Secretary of State's Procedures Manual

Your report recommends that the Procedures Manual be modified to explain more clearly that counties are required to provide my office with 1) a copy of the computer database files created for each election, 2) that these database files constitute the "computer program" described in A.R.S. §§ 16-444 and -445, and 3) that these files are not subject to disclosure under the Public Records Law.

The current version of the Procedures Manual already makes clear that computer programs filed with the Secretary of State in accordance with A.R.S. § 16-445, includes the election management software and databases. (See Manual, October 2007 at p. 86). Thus, it is unnecessary to clarify this unambiguous language. Moreover, your suggestion that the Procedures Manual be amended to clarify that these files may not be disclosed by any jurisdiction under the Public Records Law is inappropriate.

In fact, A.R.S. § 16-445 makes clear that only the program on file with the Secretary of State is not public record. It would be beyond the scope of my authority

under A.R.S. § 16-452 to extend the confidentiality set forth in A.R.S. § 16-445 to the copies of the computer programs in the possession of each county and local jurisdiction. This would require an amendment to the Arizona Public Record Law.

Your report also recommends that the Procedures Manual be amended to require the final election database and program be submitted to the Secretary of State's Office along with the election canvass. Mandating the filing of this information in the Procedures Manual is beyond the scope of A.R.S. § 16-445.

Our View: We finally agree with Brewer on something.

ARS 16-445 doesn't limit the public records disclosure from counties, nor should it. And the proposal to change state law to restrict these records goes against the public policy implications found by Judge Miller.

Basic computer science disagrees with the "security by obscurity" concepts championed by both Pima and Brewer to varying degrees. Any attempt to push "security by obscurity" in the legislature will be met with a storm of informed and qualified testimony against.

SOS BREWER'S OPINION OVERLOOKS SECURITY FLAWS IN ELECTION MACHINERY, EXAGGERATES COSTS OF SCANNING AND POSTING BALLOTS ON THE INTERNET

4. Scanning and Posting Ballots on the Internet

Your report recommends that A.R.S. § 16-621 be amended to permit counties to establish a procedure to scan and post ballots online. As I previously noted to you in my letter dated January 17, 2008, A.R.S. § 16-452 prohibits a county from establishing its own procedures for tabulating and storing ballots. As I stated, I believe this proposal involves substantial policy questions related to election administration in Arizona and that such a policy must be vetted and approved by the Arizona Legislature.

Indeed, this proposal was partially vetted by the State Senate this past February. At the Senate Judiciary Committee, you may be aware that I specifically noted that scanning and posting ballots on the internet is a very bad and costly idea. Despite the enormous costs associated with such an undertaking, no compelling argument has yet been made as to what actual benefit will come from this practice. The fact is, there is no benefit that can justify the cost and the excessive burden on county election officials, especially during a critical time when those individuals should be focusing on their critical and timely election tasks.

In the end, it appears that the only justification for this proposal is that scanning and posting ballots on the internet will provide a few "election-integrity watchdogs" a way of conducting their own review of the process. With all due respect, this is hardly justification for such a massive and costly undertaking. Let's not forget that the law already provides these individuals an opportunity to observe the tabulation process, not to mention the significant role that political party observers play throughout the entire

Moreover, the contest laws in this State already provide these "watchdogs" or any other individual the ability to question any election and to gain access to the ballots if necessary. To change the statewide policy with regard to a post-election review simply to accommodate a few individuals that have leveled unsubstantiated allegations regarding our election processes is unwarranted.

Our View: After doing so well a moment ago, Brewer falls back to "security by obscurity" and ignoring the statements made in open court by witnesses for Pima County.

With all the evidence we have on film from court trial and even the Attorney General of Arizona “Terry Goddard” publicly stated that the Diebold Election System which is used in 12 of the 15 counties in Arizona is “Critically Flawed.” This statement was recorded on video tape.

Matt Blaze PhD, University of Pennsylvania was a team leader for the California Secretary of State voting system Top to Bottom review on Sequoia's voting system. On the radio program "Voice of the Voters" August 8, 2007 he was asked:

“What is the current condition of all electronic voting equipment in United States of America?”

Answer: “Fatally Flawed” adding “We’re 3 to 5 years before anything better will be available.” Link to radio show Aug. 8: Matt Blaze, **Blaze Transcript, Audio & Podcast**

However, there is hope. The solution is transparency, transparency, and more transparency. It requires citizens to reclaim our citizenship and be involved in the process.

Matt Blaze, PhD discusses the findings of the California top-to-bottom review:

"We found significant, deeply-rooted security weaknesses in all three vendors' software. Our newly-released source code analyses address many of the supposed shortcomings of the red team studies, which have been (quite unfairly, I think) criticized as being "unrealistic". It should now be clear that the red teams were successful not because they somehow "cheated," but rather because the built-in security mechanisms they were up against simply don't work properly. Reliably protecting these systems under operational conditions will likely be very hard. The problems we found in the code were far more pervasive, and much more easily exploitable, than I had ever imagined they would be."¹³
http://www.crypto.com/blog/ca_voting_report/

Since all of Brewer-approved approaches to security are based on obscurity which protects insiders not on transparency which allows the public to verify the vote, then a low-cost “graphic scanning security patch” is the last sane solution that can verify the accuracy of the vote. Brewer simply will not confront the dire failure of the certifications processes.

Brewer is over-stating the costs for Internet distribution. The graphic scans don’t need to be individually viewable as that would mean web-programming; they can be lumped into .ZIP files and downloaded wholesale.

Note that the bill (a strike everything amendment to Arizona S.B. 1395, relating to elections; ballot processing; scanners) passed the first committee (Judiciary) 2/25/08 six “yes” to one “no” and then it died in Senate Rules (chair refused to call it). Our understanding is that Brewer’s office killed the bill. Senate Bill 1395 was permissive only, allowing Pima County to run scanners as a volunteer program but not mandating them for other counties. Despite this Brewer was bitterly opposed as were Maricopa elections officials who would have been unaffected by the bill.

Worse, Brewer’s assertion the last paragraph that states that contest laws or recounts are assurance of fair elections is incorrect as previously explained: there is NO structure in AZ law for access to the actual paper ballots under any circumstances. Even candidates cannot pay for a recount in this state.

¹³Matt Blaze PhD , Member of the California Top-to-Bottom Research Team that Found Significant Security Issues in Electronic Voting Systems. http://www.crypto.com/blog/ca_voting_report/

Why Brewer thought she could misstate matters to this degree is beyond us.

Brewer states that this is a “massive and costly undertaking”.

She must be referring to last December 19th headline in the Tucson Citizen that 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.

The estimate that we have put together gets the cost down to \$0.121 per ballot including labor and that’s if we charge all the equipment just to one election. However, if we were to depreciate all the equipment over five major elections the cost would come down to \$0.045 per ballot side or \$0.09 for both sides and I believe that we could possibly even get it lower - and at the same time and cost have the team that does this also do the post election outside audit of the process.

We propose that on election day, 10% of the precincts shall be randomly selected by drawing mid afternoon. That evening as the polls close, a special group of pre-selected audit workers will travel to those precincts with a laptop computer and small duplex scanner in a small case the would weight approximately 30 lbs. At the close of polls they will scan those paper ballots plus all spoiled ballots, the pollworkers certified report, the “Consecutive Number Register” (CNR) a.k.a. “The Poll List” provisional roster, the precinct generated Accuvote election summary result tape and also scan the zero report tapes that were generated that morning from both precinct voting machines. The rest of the ballots and documents will be graphic scanned as the post election audits are being done by high speed duplex graphic scanners that can do 125 ballots (both sides) per minute.

Now that party oversight will include getting the election databases, the graphic images scan of early ballots “Vote By Mail” (VBM) MUST BE DONE in batch numbers that match the batches that were run through the Diebold/GEMS central count scanners for all the VBM and show up under the GEMS “Administration reports” as “central count status report by deck” - this is the accounting for all VBM.

The numbers and equipment cost are all listed below and this counts the labor to also do the external audit that at the present time is done internally.

<i>quantity</i>	<i>description</i>	<i>unit price each</i>	<i>total equipment</i>	<i>special labor</i>	<i>weight in lbs</i>
40	Inexpensive laptops	\$450	\$18,000		6
40	XEROX DocuMate 600 x 1200 dpi 48bit USB 2.0 Interface Fast Duplex Sheetfed Scanner - Retail	\$669	\$26,760		8.6
40	Carrying case for both units	\$250	\$10,000		10
40	Contingency budget	\$100	\$4,000		
40	Person to do the precincts election night	\$150		\$6,000	
\$58,760	subtotal for equipment to do 10% of precincts election night				

3	Central count Duplex graphic scanners that can do 125 ballot per minute both sides; Panasonic KV-S3085 (see specification below)	\$13,911	\$41,733			
3	Inexpensive laptops computers to hook up to Central count Duplex graphic scanners	\$1,000	\$3,000			
3	Contingency budget	\$1,000	\$3,000			
560 man hours	Labor to graphic scan all the other ballots from precincts and from central count vote by mail (VBM) starting election day. 8 persons for a max of 7 days = 560 man hours. These same people would also perform the audit and would come from other department other than the election department as once done under Larry Bahill when he was Pima County Election Director and approved by political parties on ballot.	\$16	\$8,960			
	Total cost of equipment		\$106,493			
	Total cost of labor to scan and audit the election		\$14,960			
	Total estimated cost to scan with equipment and labor 450,000 ballot both sides. 900,000 images.		\$121,453			
		<i>images</i>	<i>equipment</i>	<i>equipment cost per image</i>	<i>Labor \$14,960</i>	<i>equipment and labor per image</i>
	cost to graphically scan approximately 1 million pages of images based on 1 use	1 million	\$106,493	\$0.106	\$0.015	\$0.121
5	if equipment is depreciated over 5 elections the cost would drop to	3.5mil	\$106,493	\$0.030	\$0.015	\$0.045

SOS BREWER IGNORES TRIAL EVIDENCE THAT NO ONE CHECKS: ACCUSES COUNTY OF DELAYING EARLY VOTE TABULATION TO APPEASE A FEW

4. Delaying the Tabulation of Early Votes

Another recommendation you offer is to delay tabulating early ballots until election day. Once again, you are recommending a procedure to alter the manner in which tabulation occurs throughout the State. Moreover, this new policy will

substantially delay the reporting of results for the entire State simply to appease a few individuals.

As with many of your other recommendations, your analysis with respect to early ballot tabulation is flawed and makes little sense. Such a massive change in procedure should not be done merely to accommodate the scheduling needs of political party observers. Let me assure you, the party officials are well aware of the timeline for ballot tabulation and most certainly can make observers available at any time during the entire process if they so desire.

I would suggest Pima County consider following the lead of other counties like Maricopa County when dealing with early ballot tabulation. Maricopa County provides 24 hour security surveillance of all early ballots and accommodates political party

observers to assure that they may be present at an election. Let's not forget that the law was recently amended to make it a class 6 felony to release early ballot results before election night. See A.R.S. § 16-551(C). Thus, your practice does little more than cause an unnecessary delay in releasing the tabulation results to the public.

The recommendation not to scan mail-in votes until election day stems from the Pima Elections Department getting caught peeking at and printing the results of mail-in vote totals up to 9 days pre-election (November 2006 General Election) as a clear pattern revealed from the GEMS audit log from the 2004 primaries through 2006 general election. Additionally, through testimony of several election department employees this practice goes back before 2004 primary but wasn't show on the GEMS audit log until an upgrade version of GEMS included this element of reporting.

That is fact. It's right there in the audit logs Brewer that the Pima County Board of Supervisors never looked at, and there are references to it in sworn testimony from Pima elections insiders that this data wasn't just looked at, wasn't just printed, and wasn't just passed around the office like baseball scores.

Stolen data "election results" made its way out of the elections office. Sworn testimony (depositions of Robert Evans) suggests felonies were committed regarding the theft of that data. On two occasions heavy partisan political activity in close races followed the theft of the sort of data that might trigger that activity.

Brewer's highly touted Procedures Manual did not and does not stop insider theft. Only close oversight and public records access technical experts consulting with the Pima County Democrats exposed it.

Once the data escape was exposed, the Board of Supervisors had two recourses; fire the elections supervisor, or take away any possibility they'd do this theft again. Chuck Huckleberry chose the latter.

***Our View:** We believe the proper choice was "both of the above" but in any case, Brewer is yet again ignoring bad news.*

If that information is repeatedly stolen, it will shift the political balance of power in the county and state. A political operative who knows who is winning and losing "early" *on a precinct detail level* has a tremendous advantage. If that advantage is allowed to continue unabated, we get much closer to a point that will destabilize elections. To his credit, Chuck Huckleberry realized this and backed us down from that precipice. Brewer still doesn't see how not addressing these problems leads us off the cliff's edge.

BREWER'S PRIORITIES: SPEED OVER SECURITY AND ACCURACY DISREGARDS HACKER THREAT TO MAIL-IN VOTE

5. Discontinuation of Modem Transmission Results from Polling Places

This may be the worst recommendation contained in your report. Not only will discontinuing the modem transmission of results substantially delay the reporting of unofficial results on election night, it actually introduces a major security vulnerability into the election process. This is a poorly thought out recommendation and Pima County needs to reverse this practice just as quickly as the knee-jerk decision was made to implement it in the first place.

You justify this practice because it will arguably prevent some hypothetical "hacker" from intercepting the results during the transmission and then submitting false results. This justification, however, is undermined by the fact that these results are

unofficial and do not become official until they are audited against the actual precinct machines. Any security breach would ultimately be quickly identified during the audit.

More troubling about this policy is that it actually creates a major security vulnerability by providing no independent method for memorializing the results from a given precinct. Your supposed "security procedure" apparently does not even consider that something could happen to the machines and ballots in route to the election headquarters, in which case the results of that precinct would be lost forever. Certainly the odds of some event happening during the transportation of the ballots are low, but they are no doubt far greater than the remote possibility of some hacker intercepting the results, which again would be quickly caught during the post-election audit.

It is amazing to me that Pima County insisted on unilaterally adopting this questionable practice during the Presidential Preference Election in February, despite the fact that this supposed security concern has never occurred in Arizona, is not likely to occur, and would be quickly caught by the mandatory audit that is performed on each

machine that returns to the election office from the polling site. It came as no surprise to me that Pima County was criticized for this practice because it unnecessarily delayed the election results for the entire state.

Our View: Whoever wrote this in Brewer's name yet again flunks computer security 101.

The modems open up a line of communication into the central tabulator of votes. Altering a single precinct's incoming data is, as Brewer suggests, less than useful. Tampering with the central tabulator database however is a horrific threat because the scanners that process the mail-in votes do not keep their own independent tally. There is nothing to reconcile against with mail-in votes. On election night, Brewer proposes to open those votes, *stored purely in electronic form with no paper audit trail*, to outside tampering. This is utterly insane. The precinct votes would be at some risk in the same fashion, but the mail-in vote would be wide open to unlimited hacking.

Let's assume we're talking about elections circa 1850ish. Paper ballots are going to be dropped into containers. Before that happened, people would make sure the box didn't have a false bottom, and that the lid to the ballot container couldn't be tampered with easily. These are basic concepts.

We use computers today. California Election Code 15004 provides the means for computer techs to check out the computers ahead of time to make sure there's no electronic "loose lid" or "false bottom". Brewer has a problem with that. Which is why we have a problem with Brewer. Voting is a secret process, counting votes is a public process and must remain so despite partisan opinions otherwise.

SUMMARY

In sum, SOS Brewer raises thoughtful concerns about Pima County's proposals to expand background and security checks for poll workers. Many good people might be discouraged from participation in elections as poll workers or observers or hand count auditors if they were required to submit to invasive heavy-handed security background checks.

We have no serious objections to Pima County's adoption of Brewer's instruction to discontinue the marking of test ballots by political parties outside the confines of the election department. Then again, facts are that the test ballots are stamped in large red letters with the word "TEST." And the machine tests are conducted a week before elections, but thousands of mail-in ballots are distributed up to six weeks before the election. Additionally Country Manger Chuck Huckelberry said: "If you want to

duplicate a ballot, a mail-in ballot would be the way to go."¹⁴

We continue to raise transparency objections to Brewer's policies that imply that party observers have no right to question irregularities or noncompliance with agreed upon procedures they may observe. Brewer's clearly stated opinion is that observer interference disrupts order. On the other hand we reserve the right to hold election department employees accountable for following orderly consistent and transparent procedures. We also agree that party observers shouldn't handle ballots themselves, unless they are test ballots.

We would remind SOS Brewer that there is time-honored historical precedent for checking to make sure elections were fair and honest. In elections circa 1850, paper ballots were dropped into containers. Before that people would make sure the box didn't have a false bottom, and that the lid to the ballot container couldn't be tampered with easily. These are basic concepts.

We use computers today. California Election Code 15004 provides the means for computer techs to check out the computers ahead of time to make sure there's no electronic "loose lid" or "false bottom".

Brewer has a problem with that. Which is why we have a problem with Brewer. Voting is a secret process. Counting votes is a public process and must remain so despite partisan opinions otherwise because counting votes behind closed doors is contrary to everything our Founding Fathers fought for.

Respectfully,

John Brakey and Jim March - Arizona Election Transparency Project

Jim March

Member of the Board of Directors, Black Box Voting – <http://blackboxvoting.org>
916-370-0347
1.jim.march@gmail.com

John 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

Cell 520-250-2360
AUDITAZ@cox.net

¹⁴ <http://www.azstarnet.com/allheadlines/230263>

ACRONYMS - SPEAKING THE SAME LANGUAGE NATIONALLY

Acronyms of the Election Integrity Community

HAVA	Help America Vote Act. (Orwellian-named) Hack America Vote Act – 2002 legislation allegedly “repairing” our voting process after the Florida 2000 fiasco.
EAC	<u>Election Assistance Commission</u> – created in 2002 but properly funded or even remotely functioning even on a poor level until 2006. Still not fully up to speed.
FEC	<u>Federal Election Commission</u> – sets the rules for voting system specifications VVSG.
NASED	<u>National Association of State Election Directors</u> – the group that used to do the EAC’s job managing the Federal certification process. No longer involved due to poor performance.
ITA	<u>Independent Testing Authority</u> list from Source Watch – test labs hired by the vendors to check out voting systems. Labs are managed (in theory) by the EAC.
VVSG	“Voluntary Voting Systems Guide” – blueprint for voting systems, a set of specifications the test labs are supposed to test systems to. Created by the FEC. It’s “voluntary” in terms of whether states adopt it or not – AZ is in the majority doing so and it’s not “voluntary” here.
OS	Optical Scan – general class of voting machine
OSPB	Optical Scan Paper Ballot
PDOS	Paper Ballot Optical Scan
TS	Diebold Touchscreen voting machine, paperless (older model)
TSx	Diebold Touchscreen voting machine, with optional useless thermal paper (newer model)
DRE	Direct Recording Electronic – voting systems that primarily store votes as computer data versus paper ballots.
GEMS	Global Election Management System – Diebold voting software that counts the vote county-wide. Known as a “central tabulator” class program it takes in data from everything else.
L&A	Logic and Accuracy – a pre post-election test process.
COTS	Commercial off-the-shelf software – in other words “not modified custom for voting”. On several occasions voting system vendors have passed custom software and gear off as “COTS”. Per the VVSG anything “COTS” gets less scrutiny by the labs (ITAs).
SOS	Secretary of State – in AZ the chief elections officer at the state level.
EIC	Election Integrity Committee
CNR	Consecutive Number Register
LD	Legislative District
PW	Poll Worker
PCDP-EIC	<u>Pima County Democratic Party Election Integrity Committee</u>
VVPAT	Voter Verifiable Paper Audit Trail – often known as a “toilet paper roll” when it is a crudely grafted on addition to a DRE where vote summaries are on basically cash register tape. Prone to misprints and especially jams – poor substitute for real paper ballots.

MISCELLANEOUS

- INTERPRETED CODE? Thomas W Ryan PhD “This is code that is readable by humans and modifiable by humans. This is kind of code that is often used by scientists and engineers ...because it is easily modifiable, and should be used only in an experimental environment. It should never be used in any device or system that requires security and [it] is explicitly prohibited by the 2002 Federal Election code.” Put another way: interpreted code is easy to modify in the field by elections staffers, and is present (illegally) in several voting systems – including Diebold.