

The Pima County Democratic Party offered technical expertise June 18, 2007 letter

RISNER & GRAHAM
ATTORNEYS AT LAW

100 NORTH STONE + SUITE 901
TUCSON, ARIZONA 85701

TELEPHONE (520) 622-7494
FACSIMILE (520) 624-5583
E-MAIL law@risnerandgraham.com

WILLIAM J. RISNER
*Certified Specialist in Personal
Injury and Wrongful Death*

PARALEGALS
SUSAN J. ADLER
RHONDA L. DAVIS
MANUEL LAMADRID
PATRICIA M. MATA

KENNETH K. GRAHAM
*Certified Specialist in Personal
Injury and Wrongful Death*

June 18, 2007

John R. Evans, Esq.
**OFFICE OF THE
ARIZONA ATTORNEY GENERAL**
400 West Congress Street, #S-315
Tucson, Arizona 85701-1367

Dear John:

Thank you for your prompt response to my inquiry about SAIC. We believe SAIC does not fit the profile you suggest of a neutral corporation with a reputation that would be helpful in resolving the issues in this investigation. Their suggestion of a "risk assessment" is not what is required.

If the goal is to determine whether the RTA election results were manipulated, we have a couple of suggestions. Your office is no doubt aware of the multiple security holes in the Diebold product line and, if not, I have attached four reports that deal with those issues. You may not be aware that Pima County purchased a "hack tool" known as a "cropscanner" that would enable them to tamper data before it goes into the central computer.

The Diebold precinct optical scan machines can be "electronically pre-stuffed." The Black Box Voting Report of July 4, 2005 by Harri Hursti which is attached discusses this possible method. While the memory card format in the Diebold precinct optical scanner is very obscure, a card reader sold by Cropscanner, Inc. can be used to program the memory cards and "pre-stuff" them electronically so that they will produce fake records of both the electronic vote and end-of-day tally tapes. After the publication of that report, Pima County bought one of the machines that would allow them to program the precinct memory cards. We strongly recommend that your office identify the purchase orders for this device, determine where it was stored and whether or not there were any access controls for it. This device is essentially a burglary tool for elections.

You should also note that per the BBV/Hursti report, falsifying the end-of-day precinct scanner printouts by way of hand-editing the memory card contents with a cropscanner is unusually difficult. See Appendix D of the report for what the programming looks like. It is very easy to introduce typos into the output and a pattern of such typos is cause for concern. If you then have GEMS generate the cards normally via the pre-election RTA database and

create paper tape output based on those, you will be able to determine if the typos are simply due to mistakes in configuring GEMS. If not, (in other words, if the GEMS-based output looks good), typos in the actual election tapes would be evidence of hand-edits.

We have a specific suggestion for an examination of the database relating to the RTA. Our suggestion for testing the central tabulator data files is as follows:

- 1) Write a program in Visual Basic that takes all versions of a particular election's MDB data files and produces reports as to which items in which tables have changed between iterations. In other words, for every election there is a Logic & Accuracy test beforehand, then various "snapshots" of the data as scanning progresses, then the final data file containing all votes, then the post-election L & A. Some of these will, of course, legitimately change (vote totals and audit log, maybe more) but other tables should remain identical throughout: candidate information and IDs, ballot layouts, ballot rotation information and much more. The small custom program would scan through all variations of the data and report variations by table, field and line number ("record"). A human could then check each variation and determine whether or not it's an indicator of fraud. Flipping candidate ID numbers is the single easiest hack and might be caught quickly with this process if the pre-election L&A wasn't faked or edited to match later.
- 2) In December of 2006, the Pima Democratic Party obtained a public record we will be happy to share with you: a complete directory listing of both central tabulator stations. These tell you the date/time stamps and file sizes for all the data files. When you obtain access to the same thing, compare with our December 2006 data. If file date/time/size numbers related to the RTA race have changed between 12/06 and present, it means somebody tampered with the files between those dates, probably to cover up prior misconduct. We will supply any declarations from our tech people needed to establish chain of custody on the 12/06 date/time/size data.
- 3) Find the paper results from the original pre-election and post-election L&A tests on file with the office. Take the L&A data files and run what their results should be (summary reports and cards cast reports). Compare the paper from that time period with the electronic results today. If somebody was a very careful hacker and tampered with the main data files, they'd go back and make the L&A data files match. But then the current versions of the L&A files won't match the old paper. If the old paper isn't available, the election configuration file (GEMS data file) is supposed to be recorded with Secretary of State Jan Brewer's office – you might try locating that file to determine if the county L&A data file was modified later to conform with hacking of the main vote tally data.

- 4) For each iteration of the data throughout the election that contains votes, print the "cards cast" report and build a line graph showing the progression of votes taken in. Then do the same for summary reports and graph the rising swing of each candidate over time. What you're looking for are instances of candidates "spiking" outside the normal pattern. They should progress upward fairly steadily. "Spikes" are cause for concern-look carefully at what people are doing in the elections office at the moment a "spike" happens. Do the same for other elections just to note what the patterns look like. In our experience, they vary by no more than a percent or two throughout the election.

- 5) Tally the results for the mail-in vote as compared to precinct voting. The methods available for tampering with votes varies between them. Significant disparities can be indicators of trouble, or at least a starting point for further digging. As one example: Mail-in votes are never stored on an optical scan memory card of the type the "Cropscanner" can manipulate, so that whole class of tampering isn't available for mail-in votes. It would be very possible to see tampering in one vote pool or the other leading to big shifts between them, or tampering in both but with different techniques and hence different amounts and patterns of swing.

The suggested procedure we have outlined is quite simple and does not require a corporation like SAIC. The Arizona Senate last session hired Professor Douglas W. Jones of the University of Iowa Department of Computer Science to consult with them concerning the LD20 Republican Primary of 2004. He produced a report that I have not seen but should be available to your office and would serve as an example of the kind of independent review he is capable of.

The University of Connecticut, John Hopkins University, Princeton University and the University of California at Berkeley are all quite capable of the type of independent review you are seeking.

SAIC is a huge corporation with unsolvable conflicts of interest. In 1991, SAIC was charged with falsifying data submitted to the E.P.A. Ultimately the company plead guilty to ten counts of making false statements or claims and paid \$1.3 million in fines and restitution. With regard to the electronic voting industry, we feel that SAIC has too many conflicts of interest for them to perform a truly independent examination – they have consulted on electronic voting matters for both county clients and voting system vendors. They can be described as having a vested interest in the "status quo" of electronic voting. Any proof of fraud in an electronic voting system would harm the status quo within that industry.

I was unclear if your reference to a simulation project was what our experts refer to as a "red team attack," also known as a planned intrusion attempt. I have delivered with this letter a 200 page unredacted report prepared by SAIC for the State of Maryland. That report answers many of the risk assessment questions that their offer seems to contemplate and strongly indicates that no "risk assessment" is necessary. My experts assure me that Diebold's security issues have not changed significantly since 2003, with the exception of a hard-coded password for the touchscreen voting machines (formerly "1111" nationwide). The 2003 SAIC report is still

timely.

The Ohio report that I provided to your office is an example of another type of collaborative and independent examination of an entire election.

As you are aware it may be difficult to demonstrate the RTA election was manipulated or flipped. Based upon testimony we know that one person operated the computer during the RTA ballot counting process. We have reason to believe that data may have been exported from GEMS during the counting process. That same person has been in charge of the computer ever since including more than six months after the Democratic Party asked for copies of the database over six months ago. We know that he has in fact been testing the database. Whether alterations or deletions have been made we have not been able to check.

Christopher Straub claimed in a pleading filed with the Superior Court that everyone having anything to do with the county elections computer system had a real risk of criminal exposure. I'm sure he did not mislead the court and I do not want to misquote him, so I will quote the county's pleading.:

Indeed, during the Attorney General's investigation, any attempt by counsel for either side to elicit testimony from anybody involved with Pima County's Division of Elections or the Pima County elections computer system runs a significant risk of impacting that witness's constitutional rights and eliciting an assertion of the Fifth-Amendment privilege.

(P.4, Defendant's Reply in Support of Motion for Stay of Proceedings)

Accepting the truthfulness of that assertion to Judge Miller means that caution should be exercised in collaborating with the county on the scope of an examination. They have spent months analyzing their data base as they have opposed any examination by the Pima County Democratic Party. Furthermore, that examination has been conducted by the same persons who are expected to refuse to answer questions because it would incriminate them in criminal activity. You may take responsibility for the selection of SAIC, but we are concerned that Pima County may have suggested a known compromised potential examiner for an examination of their misconduct.

We think that serious consideration should be give to a full hand count of the RTA ballots which County Administrator Charles Huckelberry claims are still in a secured facility. A hand count could be done with volunteers or hired persons from the election pool of workers. The hand count could be done in public and certainly would give the public the re-assurance they need that the vote count was accurate. Such a count would be less expensive and much more certain than a computer data analysis. An expert such as Profession Jones who has seen a lot of ballots could examine the paper ballots and readily determine the likelihood that those are the genuine ballots.

In 1997, I was an attorney in a lawsuit concerning the City of Tucson General Election for the election of three council persons. The City joined us in requesting a hand re-count of all the City's ballots. The hand recount proceeded quickly and without incident. The problem in that election turned out to be defective paper that resulted in some 9,000 votes not being counted by the machine. I mention that example because the recount of three council races on punch cards

that required determining the voters intent from "dimples" was not difficult. Certainly a yes/no election like the RTA with filled in bubbles would be much easier to accomplish.

The Democratic Party and our experts are ready to assist in any way useful to your investigation. Neither the party nor its experts have any stake in the outcome of your investigation. We have identified serious anomalies that need to be investigated and we are pleased that they are being investigated. We do believe, however, that the result should have the confidence of the public that it was not a whitewash. That is why we have made specific recommendation to accomplish that result.

In any case: we ask that you hold this document in confidence and not allow the county to review it. If there is evidence of misconduct hidden within the databases or in the paper output tapes from the precinct scanners, it might still be possible to destroy data. My clients and I are handling this letter with extreme care and to a very limited audience for review.

Sincerely,

RISNER & GRAHAM

A handwritten signature in black ink that reads "Bill Risner". The signature is written in a cursive, flowing style.

William J. Risner
Attorney at Law

WJR/pmm
Enclosures