The iBeta reports say a lot if you read it carefully and fact check it with what we have and know.

Review by John R Brakey and Jim March of the iBeta report. Friday, Dec. 28, 2007
Brakey's and March's remarks are all
indented and italicized.

Link to iBeta report:
http://www.electiondefensealliance.org/files/iBeta_Election_Forensic_Report_Pima_Co.pdf

iBeta Software Quality Assurance

Pima County Final Report

Created For:
Program Name PIMA
Final Version N/A
Client Pima County, Arizona
Project Lead Kathleen Kempley

Created By:
Project Lead William Miller
Test Lead William Miller
Date July 2007

3131 S. Vaughn Way. Suite #650, Aurora, Colorado, 80014
Phone: 303-627-1110 Fax: 303-627-1221

Table of Contents:

Executive Summary

iBeta was approached to perform a quantitative investigation for Pima County, Arizona of a specific Diebold GEMS electronic voting system version and associated hard drive data with regard to alleged vote tampering.

The investigation took place at iBeta's certified testing facility in Aurora Colorado.

iBeta received a sealed Seagate Barracuda 7200, ST3250820A, 250 gigabyte hard drive (s/n 6QEoNTQZ) from Pima County which contained four drive images in Symantec Ghost format.

iBeta staged the images for investigation and analysis using an external IDE to firewire converter. Of these images it was discovered that only two, "Item 1" and "Item 2" contained useable data and "Item 1" was 10.2 gigabytes in size while the "Item 2" image was 204 gigabytes in size.

The target file of the investigation was a Diebold GEMS database backup file called "pima consolidated 051606 EARLY DAY1.gbf" which, according to the audit log of the GEMS software was initially created 05/10/06 at 12:27:27, and then overwritten 05/11/06 at 09:56:30.

Ed: The data over-write in question can be seen in the audit logs:

```
05/10/06 08:21:41 User admin: Reset election
05/10/06 08:22:08 User admin: Printing Summary Report
05/10/06 08:38:47 User admin: Printing Summary Report
05/10/06 12:27:27 User admin: Backed up election to
      D:\Program Files\GEMS\Backup\pima consolidated
      051606 EARLY DAY1.gbf
05/10/06 12:27:38 User admin: Previewing Cards Cast Report
05/10/06 12:28:04 User admin: Backed up election to
      D:\Program Files\GEMS\Backup\pima consolidated
      051606.gbf
05/10/06 12:28:05 User admin: Closing GEMS

Now look at the next day:

5/11/06 9:55AM   User admin: User Login
5/11/06 9:55AM   User admin: Open Election:  Consolidated
      Election, May 16, 2006 (pima consolidated 051606)
      admin Host
5/11/06 9:56AM   User admin: Backed up election to
      D:\Program Files\GEMS\Backup\pima consolidated 051606
      EARLY DAY1.gbf
5/11/06 9:56AM   User admin: Printing Summary Report
5/11/06 10:06AM  User admin: Printing Summary Report
```

This from file allocation table we received by a record request.

In plain English, a backup of the day's worth of scanning on 5/10 was performed at the end of that day (12:28pm). Everything on 5/10 looks proper. The morning of 5/11 a copy of the data file was opened and there's no way to tell where it came from – it could have been copied in from other media such as a CD. One minute later the previous night's backup was overwritten – note that the filename is the same. And then somebody made two illiicit printouts of running vote totals on a precinct detail level (summary reports) effectively stealing data on how the election is going. This is all consistent with a copy of the data going home on 5/10, getting altered, being brought back in 5/11, bad data overwriting good and then printouts are made proving the hack.

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering. The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images "Item 1" and "Item 2" to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006 and the normal copy and cleanup process on July 27, 2006 in preparation for the next election.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.

   Ed: We have the file allocation tables and there are NOT 5 copies of day 1! See below. What are the time stamps for these files?

4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial "L and A" run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

During testing it was discovered that the GEMS software exhibits fundamental security flaws that make definitive validation of data impossible due to the ease of data and log manipulation from outside the GEMS software itself. [Emphasis added]

Ed: This is actually the most important item in the report. The first consultant Pima County and the AG's office tried to hire told them the same thing, and that reference back to the original paper was the sole method of reliably looking at the election's true outcome.

Ultimately, it is the determination of iBeta that the overwriting of the target file can be attributed to human error. iBeta arrives at the "human error" conclusion for two reasons:

- iBeta was unable to detect any manipulation of the 051606 event data across the multiple copies of the data discovered.

  We told the AG's office that if they were going to do data analysis, looking at how the data changed across time was the only possible route to the truth and that wasn't guaranteed. Instead, iBeta looked at multiple copies of a single "time slice".

- The basis of the investigation is that there are log entries that point to tampering - but it is far easier to remove evidence of tampering from the logs than to actually tamper with the vote totals in the Microsoft Access database that the GEMS software uses. So it does not follow that someone with the knowledge to manipulate the GEMS data would neglect to alter the log file to remove the evidence of the manipulation.

  In other words, iBeta discounts the idea of tampering because covering up the tampering evidence that IS there would be dead easy. What iBeta had no way of knowing is that the main computer operator for Pima County's elections office and the main "suspect" (Brian Crane) is barely PC competent at all. Watching his mouse

movements on-screen, it's obvious he's "hesitant" - he has to think about every action even where basic operating system commands are involved. This is the kind of guy who easily could leave traces that are otherwise easy to cover.

Summary of Testing

Setup & Planning

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering.

Test Execution

The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images "Item 1" and "Item 2" to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006.

   Only if you believe what Dr John Moffatt says and he been caught to many time covering up. On two separate occasions now he has threatened each of us (Jim March in December '06, John Brakey in June '08) with cutting off cooperation if we continued to examine past practices in the Pima elections office. He only says this to one person at a time and will likely deny it.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.

   What if all five were clones? Made from the same file? Where else could they got the 5 day ones?
4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial "L and A" run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

   Crane backs over the "day1" file of 5/10, it's gone. We're never said vote were added, we believe votes were flipped or manipulated.

Test Specifics

Test 1 – R-Studio was used to perform a drive-wide scan for deleted, partial, and ghost copy data. While RStudio did find and recover a great deal of interesting data, none of it was relevant to the investigation at hand.

- This test can be defeated by repeated loading, deleting, and defragmentation of the hard drive, which repeatedly overwrites the deleted data with parts of other files and makes recovery very difficult. Based on iBeta's observations of the drive images this defeat was not performed.

Test 2 – The date and time stamp checks of the files did turn up what appeared to be evidence of tampering as the files pertinent to the investigation showed a pattern of irregularities in either the date/time created or modified. John Moffatt did some investigation on his end and discovered that there were some issues in the backup, installation, and recovery of data during a July 20th 2006 GEMS system update followed by the normal copy and cleanup process on July 27th. This explained the oddities discovered in the file timestamps**.**

- This test can be defeated by altering the date/time stamp data for the files. There are utilities which will do this, but it appears that this was not done because the files still exhibit non-uniform dates/times. It is unlikely that that defeat was performed because if one of these utilities would have been used, there would have been no alert as all of the date/time stamps would have been sequential to the event - leaving no clue that the files had been altered or replaced.

Test 3 – Ultimately five copies of the target file were discovered or recovered. These five versions were run through a CRC32 process which is used to determine file changes at a bit level. The CRC check returned that all five of the files were identical. The CRC32 value of the target files was "FAD8C70E".

- **It is possible to defeat this test by replacing all of the copies of the target file with a prepared version.** It is unlikely that the defeat was employed due to the various modification date/time stamps on the target file – if this defeat had been deployed all of the replacements would have the same create/modify timestamp. Additionally the file residing in multiple locations on multiple computers makes this defeat very difficult as access to the various machines and knowledge of the locations would be required.

The boldface in the above paragraph tells all…

Test 4 – John Moffatt proposed a test to determine if the programming used in the 051606 event which compared the "preference" table of the initial L and A test to the various saves of the 051606 event. The compare showed that the programming never changed from the initial L and A event.

- **It is possible to defeat this test by way of replacing the preference table in all of the 051606 event data sets after the event was over.** This defeat being used is unlikely due to the modify date/time stamps of the original L and A data being from the day preceding the event and every copy of the L and A data exhibiting the same date time stamp. **A blanket replace of the entire 051606 event dataset would have had to take place to defeat this test, which encounters the same issues as Test 3.**

We had another piece of data available that we told the AG's office about: sets of complete directory listings for the servers as of December '06 and April '07.

These show filenames, file locations, timestamps and above all sizes. It was months later before the data went to iBeta. If alterations were made just before the data went to iBeta, the file sizes may not have matched the directory listings. Even when informed that this evidence existed, the AG's office never even mentioned it again.

Test 5 - John Moffatt also proposed a test to determine if any votes were added to the vote totals from an external source. This test used the GEMS software to list the decks for each segment of the 051606 event and when backing those decks out, a total of zero votes remained. This means that all of the votes seen came from the central count scanners or precinct voting machines and not some other source.

We're never said vote were added, we believe votes were flipped or manipulated!) The next line says it all!

- **As with other tests it is possible to defeat this test by ensuring that any vote modification keeps the vote totals the same. This means that if you add 1000 votes to one candidate, you subtract a total of 1000 votes from one or more other candidates.** This defeat has a low probability of being deployed based on the fact that it only works for the total number of votes. Any report run that shows the votes at a precinct level, when compared to a total votes report, will show the data modification.

Bill Risner was 100% right when he wrote a letter AG office to John Evans Aug 6, 2007 and stated:

> *"We have a "role" problem and I need your help in understanding what is going on.*

The RTA Election of 2006: Suspicions Outlined - Jim March

1) The county ran the election and had a strong interest in the outcome, going so far as to pay consultant James Barry at least $75,000 in support of the bond measure. Barry also took money from the "official" pro-RTA bond people (basically developers). $13,000 Link to testimony of James Barry, mainly to illustrate that the Pima County government had a deep, vested, and motivated interest in the outcome of the RTA election.

http://video.google.com/videoplay?docid=1282511168148207359

2) The bond measure had failed four times previously and was losing in the pre-election polls. (There was no exit poll.)

3) On the evening of the election (5/16/06) Dr. Ted Downing (a legislator at the time) noted Bryan Crane reviewing an open MS-Access manual on the table next to the central tabulator station. Brakey found op-scans breaking down and called Downing.

4) In the weeks that followed, in meetings with (among others) the Pima County Democratic Party chair (Donna Branch-Gilby), Brad Nelson refused to allow even basic oversight – such as a visual inspection to make sure that additional PC stations weren't wired into the central tabulator via the network cable clearly visible snaking under a locked door. This refusal was interpreted at the time as Nelson's practical declaration that he had an unfettered right to manipulate elections, and nothing he's done since has alleviated that apparent stance. (It's true

that since that event, John Moffatt has managed to push through some transparency measures – but all the while Nelson and Crane have systematically sabotaged Moffatt's efforts while Moffatt has acted to try and block investigations of past misconduct.)

*5) The actions of Bryan Crane on the morning of 5/11/06 have been rehashed ad nauseum. Yet the fact remains that the official story (at least the version in court on the witness stand) has Crane making **two** mistakes rapid-fire on the morning of the 11th: he over-writes the previous day's backup file (ignoring GEMS' warning about same) and then prints TWO copies of the summary report **within 10 minutes** of each other – and again, for each summary report he has to confirm his selections manually. Either mistake would be remarkable. Both happening within minutes? It **looks** like hacking. Period. The appearance is that bad data from outside the shop was brought in, uploaded, then an over-write of the previous day's good data with the bad occurred. And then two summary reports were printed moments later - to confirm a successful hack and/or in order to prove to parties unknown that the hack had occurred? **He lied about how he dose backup in the trial**. Mina Clip Testimony of Bryan Crane on the RTA and iBeta report 17 minutes:* http://video.google.com/videoplay?docid=7304338799617243809

*6) There is still a timestamp anomaly. Granted, the file "creation" and "last accessed" timestamps would have been re-written by the exchange of file servers in June of 2006 due to how Windows handles those timestamps. But our tests show that the "modified" time/date-stamp would not change due to a simple file copy operation. According to the iBeta report and associated Email traffic behind it (public records after the fact) the "early day 1" filename has a "last modified" date of the morning of May 11th 2006. But according to Email traffic back and forth to John Moffatt, the timestamp was **10:56am**.*

In December of 2006 the Democratic Party obtained a complete directory listing of both current servers. We show a timestamp for that file of 9:56am – which in turn matches the time and date that the GEMS audit log says the "overwrite" of the morning of 5/11/06 happened.

We have confirmed that if a file is created and has a "last modified" date of, say, 3:00pm, and the file is shipped across time zones by ANY means, the timestamp doesn't "auto-correct" for the new time zone. Such functionality just isn't there – the Windows file system has literally no place to record the timezone in which a file was created. So iBeta's Colorado location wouldn't have adjusted the file "last modified" time by an hour.

The implication is that somebody adjusted the file before it got to iBeta.

7) The "five files" situation. According to iBeta, they were unable to read any data off of the original pair of GEMS systems (the ones actually used on the RTA just before their retirement). From the other newer pair of systems they extracted five identical copies of the "early day 1" RTA file involved in the over-write of 5/11/06.

Our copy of the directory listings of Dec. '06 shows only two copies.

***This bolsters the possibility that the RTA data files were modified prior to being shipped to iBeta**. At a minimum, we can state that the files were being looked at and duplicated between Dec. '06 and their duplication for iBeta around June '07.*

8) Testimony under oath from lower level staff in the elections office during the public records case claimed that printing the "who's winning and losing" reports pre-election based on the mail-in data was common practice, AND that these reports made their way out of the elections office.

Printing them would be improper. Distributing them would be a felony. The system audit logs confirm habitual peeking at this confidential data pre-election from 2004 through 2006.

Conclusions:

The court has already been provided with a schedule of tests we believe should be performed on the complete data set for any given election – most definitely including the RTA '06 Special Election. We feel that some of these tests would be particularly beneficial in this case, such as checking the internal timestamps on the MS-Access tables and looking at the "vote totals flow" throughout the mail-in vote processing.