

## APPENDIX A

### CONCERNS REGARDING SHELBY COUNTY DIEBOLD GEMS CENTRAL TABULATOR ADMINISTRATION IN THE AUGUST 3, 2006 PRIMARY ELECTION

#### OVERVIEW OF GEMS TABULATOR SOFTWARE

This software can be installed on any standard PC with a Windows operating system.

The GEMS application is designed with two main pieces.

- 1) Graphic user interface file (view screens, buttons, reports, etc.)
- 2) Microsoft Access database .MDB file containing multiple tables where the actual vote totals are stored.

#### CRITICAL SECURITY BREACH

Not only was the main Diebold central tabulator found to be plugged into a county government network switch, the following unauthorized software had been installed on it:

- 1) Lexar Jump Drive encryption software.  
This would allow someone to manually transfer data between the tabulator PC and another PC using a small USB type "thumb" drive. Such drives have the capacity easily to hold the above Microsoft Access database file containing Shelby County's primary election vote totals.
- 2) PC Anywhere  
This application would allow unfettered remote access to the central tabulator to anyone connected to the county government network or the Internet.
- 3) Microsoft Office Professional (which includes Microsoft Access)  
This would allow manual editing of the Diebold GEMS database file, which is NOT password protected and bypassed by the GEMS audit logs. In fact, the "AuditLog" table itself can easily be edited. Vote totals can be altered in the "CandidateCounter" table much like editing a spreadsheet. Or, the candidate names can simply be switched in the "Candidate" table.
- 4) HTML editor software  
This indicates someone was attempting to edit saved Diebold election

summary reports, perhaps to agree with altered vote totals in the Diebold Microsoft Access database file.

### ***CONCLUSION***

Independent of voter concerns about trusting their ballot to paperless DREs, the real threat for wholesale election fraud lies with the Diebold central tabulator. If the DREs and optical scanners represent voter district "ATMs" the GEMS central tabulator is the county's "Bank".

Unless Shelby County election officials can be seen as conducting a good faith investigation as to who had access to this central tabulator PC and the above unauthorized software and who actually did the illegal install, voters in this county (and ultimately the state) can have no confidence in the integrity of the November 2006 election.

### **ACTIONS NEEDED**

- The GEMS central tabulator should absolutely NOT be connected to any network via Ethernet card, wireless network card, infrared port, USB port or modem.
- The administrator password should be changed immediately and all other user accounts with rights to install software should be deleted from the Windows Local Security Policy.
- The unauthorized software, including the Lexar Jump Drive encryption software, PC Anywhere,
- Microsoft Office Professional, and the HTML Editor software, needs to be removed **immediately** from the GEMS central tabulator.
- Just before the polls open and immediately after the polls close, all central tabulators need to be audited, especially in the Windows event logs, for the existence of unauthorized software.
- From now until after the election results are certified, all central tabulators need to be physically protected from unsupervised access by any individual, including Diebold and other voting equipment vendors. This would **especially** include the installation of any last minute software "patches" and/or hardware upgrades.

**Pages 75-76 of full document. Read entire document here:**

[https://www.tn.gov/content/dam/tn/tacir/documents/trustbutverify\\_phase1.pdf](https://www.tn.gov/content/dam/tn/tacir/documents/trustbutverify_phase1.pdf)