

Technical Committee of  
TrueVoteMD.org  
7711 Garland Avenue  
Takoma Park, MD 20912  
(info@freshaircleanpolitics.org)

State Board of Elections  
151 West Street,  
Suite 200  
Annapolis, MD 21401

October 19, 2004

During the last several months, TrueVoteMD.org has expressed concerns to the State Board of Elections about serious technical issues relating to the accuracy, reliability, and security of the Diebold voting systems scheduled to be used throughout Maryland this November. These issues relate to both the GEMS back-end servers and the AccuVote-TS DRE's.

In order to ensure that the Board of Elections, concerned Maryland voters, and the media are aware of these problems, we are sending this letter documenting our major concerns. In order to ensure that we clearly understand the Board's view of these issues, and its level of concern, we request a written response to each of the following questions be sent to the above address.

### **1) GEMS Security Vulnerabilities**

Diebold's Global Election Management System (GEMS) is used to aggregate and tabulate votes cast at local polling stations. Diebold has selected Microsoft Windows as the Operating System which supports these back-end servers and Microsoft Access as the database management system.

According to the US Government's computer security clearinghouse (The CERT Center at Carnegie-Mellon Institute), the vast majority of security breaches occur on systems using Microsoft Windows and other Microsoft products running under Windows, such as the Access database product. It is therefore critical that all security patches issued by Microsoft be applied to these servers and that network security and physical security of these servers be as sound as possible. The ease with which data values in a Microsoft Access Database can be changed once an unauthorized person gains physical access has been well publicized. This weakness becomes more alarming given the hundreds of people who have access to the GEMS back-end servers at the precinct, county and state levels.

Testimony confirmed in August of this year that the Windows security patches cannot be applied to the precinct voting machines without the Diebold software crashing. This raises a strong question about the successful application of these patches and other basic security measures to the GEMS tabulating software.

The minimum level of protection should include One-Time Passwords and the installation of monitoring tools to detect intrusion or unauthorized data changes. . Any copy of MS Access that is not directly controlled through the GEMS User Interface should be removed from the server, thereby precluding modifications to the GEMS Access DB outside of the GEMS software. As the RABA report outlines, scripts written by those with malicious intent are easy to install and execute within the GEMS system.

**Question 1** - What steps has the SBE taken to address these security vulnerabilities?

## **2) AccuVote-TS Bugs**

Voters using the AccuVote-TS machines in Maryland have experienced disenfranchisement through machine boot-up failure, machine crashes during voting, frozen screens, vote-switching, and electronic ballots which are missing one or more candidates or entire slates – which occurred in the March 2004 Senate Primary.

**Question 2** - What steps has the SBE taken to investigate these incidents, to determine the cause of failure, and to ensure these problems have been fixed?

## **3) GEMS Vote Results Integrity**

The (GEMS) version 1.18.19 we will use in the November election uses a double set of tables in the Access database to store the raw vote data, which is summed for the election results. This double set of accounting for precinct and summary data creates the structure for a second set of fraudulent data to be stored in the central database, and incorporated seamlessly in the final results. This double set of “books” raises significant questions about the reliability of the final calculations on the software reports.

Since the Board of Elections has purchased a Database (Microsoft Access) which is considered, even by Microsoft, to be insecure, it should require at a minimum, physical copies of the entire database should be made immediately before, during, and immediately after the results are compiled, without further keystrokes and under independent supervision. This table data should then be made available for public inspection of each of the three copies, and each tabulator hard drive should be sequestered by authorized Board staff for 24 months, the standard in other states for vote record retention. In addition, the entire set of raw data by precinct should be made available in electronic form to the public.

**Question 3** - What steps has the SBE taken to address the problem of double sets of vote data within the GEMS tabulating software?

#### **4) Lack of a Performance Quality Control System**

In order for actual polling experience to be captured and used to evaluate and improve the system, it is necessary that formal quality control procedures be defined and implemented.

Currently, there are no procedures in place nor are any resources provided for local polling places to document system problems for later evaluation and system improvement. Indeed TrueVoteMD.org is trying to fill this gap with its poll watching effort.

**Question 4** - What steps has the SBE taken to provide a quality control system to document performance issues during use?

#### **5) Back-End Disaster Recovery**

Disaster recovery at the GEMS level should include, at a minimum, redundant data storage such as that provided by "RAID" (Redundant Array of Inexpensive Disk) or mirroring , which allow continuous operations in the event of a single disk failure.

According the *Lessons Learned* report published by the Maryland Association of Election Officials (MAEO), as of May 2004 there was no disaster recovery plan in place.

Consider the consequences of an election-day system crash in the Diebold environment where there is no paper trail and no tested, reliable disaster recovery procedure in place.

**Question 5** - What disaster recovery procedures has the SBE implemented to safeguard the vote totals for the November 2, 2004 Election?

#### **6) Screen Misalignments**

Screen misalignments between the display and the touch position detection are a common problem in touch screen displays, and have been a persistent problem with touchscreen DRE's, such as a Dallas, Texas election in 2002. The misalignment causes the voter's selection to be switched to a different candidate. This is the probable cause for the switching of votes from Cheryl Kagan, candidate for the Maryland House of Delegates in 2002, to another candidate, as verified by the chief election judge (a former attorney for the US Justice Department). The solution to this problem is proper maintenance and thorough testing.

**Question 6** - Have procedures have been implemented for verifying the screen alignment of each machine prior to shipment to the polling place and for testing each machine after shipment to the polling places and assembly, to ensure that the screen is properly aligned with the touch position detectors?

## **7) Procedures for Response to DRE Failures**

According to the *Lessons Learned* report published by MAEO, when serious problems were reported for Diebold AccuVote-TS machines, technicians representing themselves as Diebold employees entered polling places, made system changes and repairs, and departed without leaving any documentation describing the problems they found or the changes they made to the machines.

**Question 7** - What procedures has the SBE put in place to:

- a) Respond in a timely manner when local election officials report AccuVote-TS machine failures?
- b) Provide local election officials with the means to identify certified Diebold technicians?
- c) Require that Diebold technicians provide local election officials with documentation of their activities?
- d) Create permanent audit logs for an independent record of all changes made on or after election day?
- e) Ensure all Diebold technicians are properly credentialed and easily identifiable by Board of Election officials?
- f) Secure logs from the GEMS server?

## **8) Emulation Attacks Through the Smart Card Port**

For a professional attack intended to change the election outcome, there is an additional vulnerability provided by the smart card reader in each machine. The plans for this smart card electronic interface are on the Internet for public view, including a parts list. This interface can be used legitimately for developing and testing smart card-based systems, and used illegitimately for attacking a variety of systems including voting machines.

An emulation of the smart card can create an interface that allows new software code to be inserted into the machine to change votes or other functions. Or, the emulator can just change the vote counts, leaving no evidence of a simple data change. The attack can be carried out by a voter on election day to change recorded votes, or by an insider prior to election day after all integrity checks have been performed. The attack exploits a vulnerability in the driver software that reads the smart card. That software is likely Commercial Off-the-Shelf Software (COTS), and thereby exempt from state and federally-required inspection by the

Independent Testing Authority. This vulnerability has twice been brought to the attention of election authorities in Maryland.

**Question 8** - What procedures has the SBE put in place to:

- a) test if the AccuVote-TS driver software has this exploitable vulnerability to emulator smart cards?
- b) implement procedural protections against this hacker vulnerability, both prior to and during election day?
- c) prevent this kind of attack in the future beyond procedural protections?

## **9) In Case of Machine Failure, Paper Ballots in Every Precinct**

On October 9, 2004, a federal judge set a trial date for a lawsuit brought by Congressman Robert Wexler (D-FL) charging that the procedures used by the state of Florida to recount touch-screen results in close elections are unconstitutional. Representative Wexler urged the state to require a paper record of every vote cast on this type of equipment. Similarly, the Maryland case of Linda Schade et al v. Linda Lamone et al seeks a voter-verified paper audit trail. The RABA report commissioned by the state legislature clearly states that a voter-verified paper audit trail is essential. Nevada has recently implemented a state-wide DRE system with a federally-certified and state-certified voter-verified paper audit trail. California will allow any person desiring a paper ballot to use one without restrictions in this November's general election.

Expressing concern about power outages, Maryland State Delegates in a February 2004 House Ways & Means committee hearing asked Linda Lamone whether the Board of Elections had contingency plans which address problems caused by power failures at polling places. In response, the State Election Administrator testified that paper ballots would be available in every precinct to be used if the Diebold DRE's became inoperable.

However, in the March primary three weeks later, the state had not provided back-up ballots, as was demonstrated at Bates Middle School. Several months later, in the September 2004 District 2 election in Prince Georges County, voters were again disenfranchised due to lack of back-up paper ballots at polling places which suffered machine boot-up failures. TrueVoteMD.org received reports from Prince George's County voters that they repeatedly asked election officials for back-up paper ballots because the DRE's were not working - none were provided.

TrueVoteMD.org urgently requests that back-up paper ballots are provided in every precinct in case of machine failure for this November election.

**Question 9:** Will back-up paper ballots of any kind be available in cases of machine failure, as has happened in each Maryland election to date with Diebold DRE's?

Thank you for your consideration. This does not represent all of our concerns but is a list of priority issues, especially of the TrueVoteMD.org Technical Committee, comprised of computer professionals from around the state. Please respond by mail to Jim Johnson, Chair TrueVoteMd Technical Committee at 7711 Garland Avenue, Takoma Park, MD 20912.

Working to Get Every True Vote Counted,

Representatives of the TrueVoteMd Technical Committee  
(years of professional work in information technology as indicated)

James Johnson, Chair [jamesj@mckpr.com](mailto:jamesj@mckpr.com) 301-589-3434 ext 160

member of Institute of Electrical and Electronic Engineers (IEEE) P1583  
Standards Working Group on Voting Equipment  
and Association for Computing Machinery  
(30 Years)

Stanley Klein, member of IEEE P1583 Standards Working Group on Voting  
Equipment  
and Association for Computing Machinery  
(39 years)

Richard Tatlow (40 years)

George Gluck, member of Association for Computing Machinery  
(37 years)

Bill Wallace (37 years)

Brian Judy (20 years)

Ross Mohan (18 Years)

John Straub, PhD (13 years)

Nancy Wallace (10 years)

cc: Governor Robert L. Ehrlich, Jr. (via fax and regular mail)  
Maryland State Legislature (via email)  
Maryland Association of Election Officials (via email)