



TEXAS DEPARTMENT OF INFORMATION RESOURCES

P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.state.tx.us

Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

February 21, 2006

LARRY A. OLSON
*Chief Technology Officer
State of Texas*

— ♦ —
DIR BOARD OF
DIRECTORS

— ♦ —
WILLIAM TRANSIER
Chair

LARRY R.
LEIBROCK, Ph.D.

M. ADAM
MAHMOOD, Ph.D.

THE HONORABLE
DEBRA MCCARTT

KEITH MORROW

CLIFF MOUNTAIN

BILL WACHEL

ROBERT L. COOK
Ex Officio

ADAM JONES
Ex Officio

BRAD LIVINGSTON
Ex Officio

Ms. Ann McGeehan
Deputy Assistant
Office of the Secretary of State
1019 Brazos Street
Austin, TX 78701

RE: Examination of Voting Hardware and software from Diebold Election Systems

Dear Ms. McGeehan:

I attended a scheduled examination January 19, 2006, at 8:30 pm for the purpose of examining the Global Election Management Systems (GEMS) software and changes to Ballot Station firmware produced by Diebold Election Systems. The report below summarizes my findings.

Hardware/Software Version	Date Previously Certified
GEMS 1.18.24	6/29/2005
Accuvote-TSX w/4.6.4 firmware	3/21/2005
Accuvote-TX R6 w/4.6.4 firmware	3/21/2005
Voter Card Encoder 4.6.1	3/21/2005
AccuVote-OS Optical Scanner 1.96.6	12/2/2004
Key Card Tool 4.6.1	12/2/2004
Express Poll 4000 1.1.5	None

Results of the examination

This examination is to certify upgrades of GEMS components to 2002 voting standards. The upgrades include a few minor bug fixes and cosmetic/documentation changes to the source code. In addition, the vendor noted that a few hardware changes were made to comply with 2002 standards.

The vendor provided a change list for most of the products at this examination. Some of the fixes for past versions appear to correct potentially serious problems. This raises concerns about the vendor's development methodology that are addressed later in this report.

The vendor noted that they are migrating to a more robust SQL database for GEMS to enhance performance and security. The database is currently not encrypted in the central count server, but is encrypted on voting machines, data cards, and in transit during modem transfer to GEMS. It is recommended that this migration be accomplished as soon as possible, and be made available to all current customers.

In addition, the vendor noted that they do not have a facility to accumulate all the logs from individual voting devices into a single database. It would seem that that such an approach would provide a unified audit trail to help detect potential irregularities and attacks. Further, making such a log publicly accessible after an election would provide a deterrent to tampering with the voting devices.

The vendor introduced the Electronic Poll Book – Express Poll 4000. This is a voter registration and verification system that includes numerous features to allow pollworkers to verify voters, direct them to proper voting locations, and track who has voted. This is a standalone system independent of their voting devices. It is not necessary to conduct an election using any of the other Diebold equipment. However, it can be used to create voting cards, and to record that a voter was issued a ballot. Under these circumstances it does not seem that the device needs certification as a voting device.

Voter Verified Paper Trail printer

The vendor demonstrated the Voter Verified Paper Trail (VVPT) printer attachment. The printer is not required for voting in Texas although some jurisdictions have asked for it. The printer module appears to be well designed, and Diebold has always had one of the best physical and user interface designs among all DRE systems.

It is more difficult to move a VVPT machine to curbside for voting because it is somewhat bulkier and heavier than the current devices. The printer can be disconnected from the DRE, but cannot be reconnected to the machine without shutting the device down and restarting it.

The vendor said jurisdictions have generally considered the electronic record to be the official vote, while the paper version is only used for vote verification. This would seem to be a very sensitive policy decision that should be established through rule or statute before VVPT is accepted for use in general elections in Texas.

Note that the same problem obtains if duplicate electronic records within a single DRE have different vote records. For instance, some vendors have as many as seven different and redundant records of the votes, so it may be important to establish which medium contains the official record. While it may be extremely difficult to compromise a DRE before or during an election, it may be much easier to corrupt one or more of the redundant media after the polls close. This would cast doubt on the accuracy and reliability of the electronics, and make a recount a tug-of-war among interest groups that favor one recording media over another.

It should also be pointed out again that VVPT also creates anonymity issues. It is possible that pollworkers could direct particular voters to specific voting machines in a particular order to track their votes by examining the paper records after the election.

Voting tests

Voting was conducted on the DREs, and they appeared to perform as the vendor claims. A single DRE is used to accumulate totals from all other DREs, then modem them to a central count. The vendor did not have the proper equipment to demonstrate the modem functionality during the exam, although they demonstrated it later to SOS staff.

The optical scanner had problems typical of all vendors' optical scan devices – light marks, stray marks, and ballot defects affect the accuracy of the count. However, within the published parameters the scanner appeared to count votes correctly, and the GEMS central office software accumulated and tallied the votes correctly.

However, Pennsylvania recently decertified the AccuVote OS Model D optical scan precinct reader 1.96.6 because they found it contains an interpreter with which vote tabulation can be manipulated at the precinct level. This appears to violate federal standards that prohibit interpreted code in voting systems under most circumstances. The full report on the decertification can be found at <http://www.hava.state.pa.us/hava/cwp/view.asp?a=1283&Q=445840>.

Concerns about the vendor's development environment

The vendor was questioned about its software engineering methodology, especially the systems specifications, design, testing, and quality assurance processes. The representatives answered that they used Bugzilla to track bug reports, and CVR. When asked pointedly about specific QA procedures such as peer code reviews, they noted that they did not use such processes.

The vendor also claims to be ISO 9001 certified. After the exam they forwarded an Adobe Acrobat (PDF) copy of their certification that was awarded in 2000. There is no evidence that the company has not been recertified or audited since that time. Further, the ISO 9000 audits focus mostly on how organizations document the results of their processes, not on the quality of the processes themselves. Thus this certification does not seem to add any significant information about the quality of their development processes.

From the sparse answers the vendor gave to this line of questioning, it is not possible to evaluate the rigor of their development methodology. In view of the issues that have come to light with the security of their systems, this would appear to be an area that should be probed in greater detail.

Recommendations

It is requested that at the next examination the vendor provide a comprehensive presentation of their development methodology(ies) including developing system specifications, design, coding, testing, quality assurance, documentation, IV&V and security within the DRE and GEMS, as well as within their development environment.

At this time, the Department of Information Resources (DIR) finds no objections to certifying all components of the system as presented at this examination except for the following:

- Express Poll 4000
- AccuVote OS Model D optical scan precinct reader 1.96.6

Respectfully,



Nick Osborn
Systems Analyst