Voting System Examination
Diebold Election Systems

Prepared for the
Secretary of State of Texas

James Sneeringer, Ph.D.
Designee of the Attorney General

This report conveys the findings of the Attorney General's designee from an examination of the equipment listed below, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date	January 19, 2006
Report Date	February 24, 2006

Components Examined

Component	Version	NASED Number
Global Election Management System (GEMS), Central Count	1.18.24	N-1-06-22-22-002
AccuVote-TS R6 Voting Station	4.6.4	N-1-06-22-22-002
AccuVote-TSX Voting Station, with optional AccuVote Printer Module (AVPM)	4.6.4	N-1-06-22-22-002
AccuVote-OS Optical Scanner (Model D)	1.96.6	N-1-06-22-22-002
VC Programmer	4.6.1	N-1-06-22-22-002
Key Card Tool Utility	4.6.1	N-1-06-22-22-002
ExpressPoll 4000	1.1.5	N-1-06-22-22-002
ExpressPoll 2000	1.1.5	N-1-06-22-22-002
Voter Card Encoder		N-1-06-22-22-002

Voting

Election Setup	PCMCIA card. Nothing is pre-programmed in the terminals; all the election information is in the PCMCIA card.
Zero-total report	On the thermal printer.

Authorization to vote / Ballot selection	Voter cards (PCMCIA cards), which authorize voting, are generated by • A handheld Voter Card Encoder, which can handle up to 8 ballot styles, • A laptop running VC Programmer software, • An ExpresPoll 2000 or ExpressPoll 4000 electronic pollbook, or • An AccuVote R6 (occasionally). A manager card is used to authorize a machine to generate voter cards. The voter cards are automatically erased after voting, so they cannot be reused. The manager card and password authorize someone to perform any operation that the R6 is capable of, including clearing elections (although the last copy is never erased). There is no hierarchy of management functions. The ExpressPoll 2000 or ExpressPoll 4000 can keep voter registration records and determine who is authorized to vote and which ballot each voter should receive. It can also create PCMCIA cards to authorize voting.
View / Vote	LCD display / touch screen
Vote Storage	Internal flash memory and on the PCMCIA card.
Precinct Consolidation	Any R6 can accumulate results from other R6 devices in the same precinct, and forward all the results to election central in a single modem call. The R6 has a real-time audit printer.
Transfer Results	PCMCIA cards or a modem.
Print precinct results	On the thermal printer
Straight party / crossover	Yes. Canceling a straight-party vote does not affect any crossover votes.
Provisional Ballots	The poll worker can designate a ballot as provisional and enter a number that will identify the ballot so it can later be included in or excluded from the count. The voting station will verify that the ballot ID is a valid one, preventing most entry errors, but duplicates are not detected unless the same voting station is used.
Voter-Verified Paper Audit Trail (VVPAT)	Yes, with the optional AccuVote Printer Module. For privacy, the VVPAT is maintained on a paper tape that is automatically wound onto a spool with a one-way clutch that does not permit viewing after verification by the voter. However, privacy can be compromised if someone at the polling place keeps a record of the order in which people vote on a particular machine, since the VVPAT records the ballots in order. For easier counting, each paper vote record is followed by a bar code containing its votes. If the voter rejects the printout, a "Void" message is printed instead of the bar code. The voter can only reject the printout twice.
ADA	Yes, but ADA capability is verified separately by the Secretary of State's office, so it was not demonstrated to the examiners.
Curbside Voting	Curbside voting with the optional VVPAT requires taking the entire voting station (not just the tablet) to the curbside. This is awkward, but acceptable.
Note	Each R6 is an independent stand-alone system, which cannot communicate with other stations or election central except when the polls are closed.

Election Setup / Tabulation

Results Storage	Encrypted, proprietary database on the hard drive.
Tamper Resistance	The OS is locked down during tabulation and the data is encrypted.
OS access	None during tabulation.
Real-Time Audit Log	Yes.
Transaction Processing	They use the transaction processing/rollback feature in the Microsoft Jet database to ensure that data remains consistent in the database.

Changes

- Added the ExpressPoll 2000, ExpressPoll 4000, and VVPAT on the AccuVote TSX
- Added a "Central Administrator Card." Now, only someone with such a card (which is not normally given to precinct workers) can do risky operations, such as delete data or zero vote totals.
- All products now qualified to 2002 standards
- Upgraded to AES128 encryption
- Bug fixes

Conditions

1. Although Diebold's support for provisional ballots worked correctly, multiple provisional ballots with the same identifying number are accepted if they are submitted to different voting stations, because the stations are not connected during voting and therefore cannot detect duplicates. Diebold recommends the use of preprinted labels with unique provisional ballot IDs.
   Recommendation. The use of such preprinted labels should be a condition of certification.
2. Diebold recommends that only the necessary Diebold computers be allowed on the local area network (LAN) with the GEMS computer, for security reasons.
   Recommendation. They are correct, and this should be a condition of certification.

Comments

3. Diebold has been certified to comply with ISO 9001:2000 standards for the design, manufacturing and servicing of voting systems. This is a large factor in Diebold's favor.
4. In many respects, Diebold has done a good job of implementing the VVPAT. The voter cannot walk out with the paper record, but can easily verify it. Also, rejecting a printout does not require starting over, bar codes are provided for easy recounting, and bar codes are only printed on accepted printouts.

Concerns

5. For all its advantages, Diebold's VVPAT system has one inherent weakness. There is a possible compromise of privacy, because the paper records for each voting station are stored in the order that people vote. For example, if everyone in a precinct votes on a single DRE, comparing the VVPAT tape to the voter sign-in log would reveal how people voted. Even with multiple machines, a poll watcher could record the order in which people vote on a given machine.
   Recommendation. If the VVPAT tape is an open record under Texas law, then the Diebold VVPAT appears to violate Texas law, and I recommend against certification. If access to the VVPAT tapes can be carefully controlled, then conditional certification may be possible, but the procedures should be though through very carefully. The sealed canisters containing the paper records should never be opened in the precinct, and possibly never be opened at all unless a recount is required. If they are opened, the environment should be carefully controlled, and it should not be done by people who worked in any affected precinct.
6. Although it was not discovered during the exam, it has come to this examiner's attention that the AccuVote OS Optical Scan Model D can be compromised by a procedure known as the "Hursti exploit," which is briefly described in the following quote from page 7 of *Examination Results of the Diebold Election System's AccuVote TSX Electronic Voting System, OS Optical Scan Units and GEMS Election Management Software*, published by the Pennsylvania Department of State on December 22, 2005, and available at http://www.hava.state.pa.us/hava/cwp/view.asp?a=1283&Q=445840:

   > **In June 2005, Finnish security expert Harri Hursti demonstrated that the memory card used in the AccuVote OS units can contain executable code, and that furthermore, the scanners will execute the code if it is present. Hursti was able to use this fact to program a memory card so that it (1) contained counters that were not zero and, in fact, had counters with negative vote totals; (2) produced a zero tape nevertheless; and (3) used the negative counter values to subtract votes from candidates and positive counter values to add votes to candidates, which resulted in a complete manipulation of the election. Note that if the sum of the negative and positive counter values are zero, the total number of votes tallied will exactly match the total number cast, and nothing will appear to be amiss. Hursti was able to disguise the behavior so it would not be detected in pre-election or post-election testing. (A manual recount would reveal this.)**

   Additional information is available from the State of California at www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf.

   Recommendation. The AccuVote OS Optical Scan Model D version 1.96.6 should be temporarily certified with the condition of strict procedures to protect the memory cards from tampering, both before and after the election, as suggested in the report from

California on page 4, in the section entitled "Strong control over access to memory cards for the AV-OS." This is only a short-term solution; Diebold should fix this problem.
Note 1. Enough information is already on the public record to allow a skilled person to exploit this vulnerability, so dealing with this problem is a matter of some urgency.
Note 2. There have been reports that the AccuVote OS Central Count optical scanner and the AccuVote TSX DRE also have this vulnerability. However, there is much less risk associated with these devices, and this problem should not cause certification to be withheld at this time, although new crypto keys should be required, as recommended in the California report.

7. The precinct totals printed at the polling place do not show the number of provisional ballots cast. This number can be calculated by subtracting the values of two of the totals that are reported, but it is confusing. An election worker might easily think that the machine was broken, rather than realizing that the difference is due to provisional ballots.
   Recommendation. The number of provisional ballots should be printed on the tape, and Diebold should review the tape messages for clarity (especially the way the results are labeled) in light of the new provisional ballots.
8. Although GEMS does not permit access to the operating system during counting, this is implemented using a feature of Microsoft Windows, and can be turned off by anyone with Windows administrative rights, provided GEMS has not been started. Once GEMS has been started, it is no longer possible to defeat this. Diebold has addressed this by restricting administrative rights, but that is not sufficient in my opinion.
   Recommendation. GEMS should refuse to tally real votes unless operating system access is actually disabled. (For example, when GEMS starts, it could check that the proper Windows settings are actually in force, so that OS access is known to be actually disabled. If they are not in force, GEMS could refuse to run.) Conditional certification should be granted for approximately one year, with the condition that this be fixed and re-inspected within that time.
9. The Voter Card Encoder should have been listed on Form 100 and should have a version number.
10. ExpressPoll 2000 should have been listed on Form 100.