

Voting System Examination

Hart InterCivic

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, pursuant to Title 9, Chapter 122 of the Texas Election Code, section 122.036(b).

Examination Date	May 27, 2004
Report Date	June 19, 2004

Component	Version	NASED Number
Ballot Origination Software System (BOSS)	3.4.0	N-1-04-22-12-003
Ballot Now: Paper Ballots	2.3.0	Pending
eSlate Voting Station	2.0.13	N-1-04-22-12-002
Judges Booth Controller (JBC)	2.2.1	Pending
Tally Vote Tabulation System	3.2.0	N-1-04-22-12-002
Rally Vote Transfers to Tally	1.2.0	N-1-04-22-12-002

Improvements

- Provisional ballot support.

Notes

- Hart is ISO 9000 certified, so their engineering processes are certified by an external agency. This is a very positive factor.
- Hart sells a number of scanners, which were not presented for certification, presumably because they are unchanged.
- Hart automatically assigns recall numbers to provisional ballots and prints the recall number to avoid transcription errors; this is preferable to manually assigning them, as some systems require.
- On Tally and Rally, the real-time audit log did not work properly in May, 2003, because the system continued to function when the printer was disabled. This was fixed and confirmed by the Secretary of State in June, 2003.
- This is an excellent system with very few problems.

DRE System: eSlate Precinct Voting System (PVS), including Judges Boot Controller (JBC)

Election Setup	PCMCIA card (Mobile Ballot Box, or MBB) created with BOSS election setup software
Zero-total report	On thermal printer
Authorization to vote / Ballot selection	A four-digit authorization code is issued to each voter on a tape printed at the election judge's controller
Provisional Ballots	The system allows ballots to be designated as provisional and automatically assigns a recall number to each one and prints it out. Each provisional ballot can later be included in the tally or can remain excluded.
View / Vote	LCD display / selection wheel and keys
Vote Storage	Flash memory (MBB)
Precinct Consolidation	Not applicable. Precinct results are all accumulated together in the judge's controller.
Transfer Results	Flash memory (MBB) used to send to Tally software. Protected by a CRC on each vote record.
Print precinct results	On thermal printer
Straight party / crossover	Yes. A warning is given if a straight party vote cancels a crossover vote that has already been selected. This prevents straight-party voting from having an effect the voter did not intend.

Tabulation and Transmission Software: Tally and Rally

Results Storage	Sybase SQL Anywhere
OS access	Not permitted during tabulation. You can restart the system, but it is logged.
Real-Time Audit Log	Yes, but it did not work properly. See below.
Data Integrity	Sybase SQL Anywhere implements transaction protection (using a log file), so that either all the data in a transaction is posted, or none of it is.
Transmission	The Rally system can be placed in a regional center to collect results and forward them to the central counting location. No tabulation is done. It merely accepts precinct results and forwards them. All transactions are logged.

Ballot Printing Software: Ballot Now

Election Setup	PCMCIA card (MBB) created with BOSS election setup software
Notes	<ul style="list-style-type: none"> • Ballots produced on demand • Each ballot has a serial number and a bar code, which prevents ballots from being counted twice by the Tally software.

- | | |
|--|--|
| | <ul style="list-style-type: none">• Especially good for absentee ballots |
|--|--|

Concerns

1. Tally and Rally can operate on a local area network. Networking allows multiple people to work simultaneously and can provide the redundancy that is required in election systems. However, it also creates a security risk by potentially allowing anyone on the network access to the election data. In short, physical security of the entire network is the only satisfactory answer.

Recommendation: Certification should carry the condition that physical security must be provided for all the computers on the election system network and for all connection points to that network, even if no computer is connected. The use of the computers on the election network for any other purpose should be forbidden when election data is present.