# 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** | January 17-18, 2008 |
| **Report Date** | March 3, 2008 |

| **Component** | **Version** | **NASED Number** |
|---|---|---|
| Ballot Origination Software System (BOSS) | 4.3.13 | N-1-04-22-22-006 |
| Ballot Now: Paper Ballots | 3.3.11 | N-1-04-22-22-006 |
| Tally (Vote Tabulation System) | 4.3.10 | N-1-04-22-22-006 |
| Rally (Vote Transfers to Tally) | 2.3.7 | N-1-04-22-22-006 |
| Servo (Warehouse Software) | 4.2.10 | N-1-04-22-22-006 |
| Electronic Crypto Module (eCM) | 1.1.7 | N-1-04-22-22-006 |
| Judges Booth Controller (JBC) | 4.3.1 | N-1-04-22-22-006 |
| eSlate Voting Station | 4.2.13 | N-1-04-22-22-006 |
| eScan Precinct Scanner | 1.3.14 | N-1-04-22-22-006 |

## Improvements

- Hart software before System 6.0 has been decertified, which means that Hart systems in Texas are no longer vulnerable to attacks using ResetPVS, an old utility that clears all the votes on a JBC, MBB and eSlates, but which doesn’t work with currently certified Hart systems.
- Hart has changed the JBC/eSlate so that the password to close the polls early is one that is not normally give to poll workers. They did this to prevent poll workers from practicing poll closing on the morning of elections day, because closing the polls is permanent and results in taking the station out of service for the day.

## Notes

- Hart has recently developed techniques to achieve and verify a NIST hardened configuration, but they are not currently in use because they have not yet been certified. I highly recommend that these be introduced as quickly as is practical. Since this is not closely coupled with the Hart software, the Secretary of State should permit an expedited approval process, possibly involving only two technical examiners.
- The overall system is referred to as System 6.2, even though the version numbers of the individual components do not contain 6.2.
- Hart is ISO 9000 certified, so their engineering processes are certified by an external agency. This is a very positive factor.

## DRE System: eSlate Precinct Voting System (PVS), eScan Precinct Scanner, and Judges Boot Controller (JBC)

| | |
|---|---|
| Election Setup | PCMCIA card (Mobile Ballot Box, or MBB) created with BOSS election setup software |
| Zero-total report | On a thermal printer, which is found on both the Judge's Booth Controller (JBC) and on the eScan. |
| Authorization to vote / Ballot selection | For the eSlate, 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, automatically assigns a recall number to each one, and prints it out. Each eSlate provisional ballot can later be included in the tally or can remain excluded. Recall numbers are automatically assigned to provisional eSlate ballots and the recall numbers are printed, so transcription errors are avoided; this is preferable to manually assigning them, as some systems require.<br>With the eScan, provisional ballots must be handled with a manual envelope system, where ballots are not scanned until they are accepted. |
| View / Vote | For the eSlate, LCD display / selection wheel and keys |
| Vote Storage | Flash memory (called a Mobile Ballot Box, or MBB) |
| Precinct Consolidation | Not applicable when only eSlates are used, because precinct results are all accumulated together in the Judge's Booth Controller (JBC). If both eSlates and eScans are used in the same precinct, consolidation is done on one of the eScans, but only for the purpose of creating the precinct report. All the MBBs from both eSlates and eScans are carried to election central. |
| Transfer Results | Flash memory (MBB) used to send to Tally software. Protected by a hash on each vote record. The Electronic Crypto Module (or eCM, a USB dongle) must be present for Tally, BOSS, Rally, Ballot Now or Servo (warehouse software) to create or use a Mobile Ballot Box (MBB). |
| Print precinct results | On thermal printer. There is a thermal printer on the JBC and on the eScan. If both are used in the precinct, the precinct report is printed on the eScan. |

| | |
|---|---|
| Straight party / crossover | Yes. Also, 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. |
| Precinct Scanning | The eScan precinct scanner integrates with the precinct system. Results from the JBC can be placed on an MBB and plugged into the eScan, which then produces the precinct report with totals from both the DREs connected to the JBC and the eSlate precinct scanner. |
| Voter-Verified Paper Audit Trail (VVPAT) | Yes, there is an optional VVPAT. 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. The voter can only reject the printout twice. ***Important Note:*** Although Hart has a VVPAT, VVPATS are not required in Texas, and there are no standards for their use in Texas. |

## Tabulation and Transmission Software: Tally and Rally

| | |
|---|---|
| Results Storage | Sybase SQL Anywhere |
| OS access | Not permitted during tabulation, except as noted under concerns. You can restart the system, but it is logged. However, see Concern number 1 below. |
| Real-Time Audit Log | Yes. |
| 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 data and forwards it. All transactions are logged. |

## Ballot Printing Software & Ballot Scanning: Ballot Now & BOSS

| | |
|---|---|
| Election Setup | PCMCIA card (MBB) created with BOSS election setup software |
| Ballot Scanning | • BOSS can scan ballots, allow manual interpretation of any undervotes or overvotes, and create Cast Vote Records (CVRs) that can be input into Tally. |
| Notes | • Ballots are produced on demand<br>• Each ballot has a serial number and a bar code, which prevents ballots from being counted twice by the Tally software.<br>• Especially good for absentee ballots |

## Verification of the Software Version

1. On January 17, Steve Berger and I, with telephone help from Tom Watson, verified using hash codes that our installation CDs were the same as those tested by Ciber, the national test lab used by Hart. Then we installed the system from the CDs, thus verifying that the software we tested was the same as that tested by Ciber. We used a Knoppix CD from NIST to generate the hash codes, and Excel to compare them.
2. After installation, we also attempted to verify that the hash codes of the installed files matched those from the National Software Reference Library (NSRL). The installation installed files on one computer and 135 on the other. Of those, only 326 from the one computer were in the NRSL and only 110 from the other. On both installations, a large number of files could not be verified.

## Concerns

1. During the exam, we discovered a way to access the operating system and delete or run other programs while Tally (the central count program) is tabulating results. Under the rules of the Texas Secretary of State, this is not permitted. I see no benefit to revealing in a public document how this can be done, but Hart is aware of the problem, and more information is available to them from myself or any of the technical examiners.
   **Recommendation:** The system should be certified on the condition that the problem be fixed and the system recertified within a reasonable amount of time, say a year.
2. If the same ballot is scanned by an eScan and by Ballot Now, it will be counted twice. This is not a big enough problem to prevent certification, since many systems will count ballots twice if they are scanned twice. However, since the Hart system normally refuses to count the same ballot twice, election officials may become somewhat lax about enforcing procedures to prevent this.
   **Recommendation:** Hart should warn counties of the importance of keeping eScan ballots separate from Ballot Now ballots, so they are not scanned twice, and tell them why.
3. Hart'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. If the VVPAT tape is an open record under Texas law, then the Hart VVPAT may violate Texas law.
   **Recommendation.** This problem needs to be considered and addressed by the Secretary of State and the Legislature. This type of VVPAT is only acceptable if the VVPAT tape is not an open record, and procedures are in place to protect the privacy of the tape. Possibly the tape would only be opened in the event of a contest, and only under controlled circumstances. Also, standards and procedures should be developed for VVPAT use in Texas.
4. Some JBCs in Tom Green Country were accidentally cleared before they were backed up. Clearly this was a human error, but election systems should do everything they can to prevent human error. For example, since the JBCs presumably knew that they had not been backed up, it might be possible for them to refuse to reset or at least give a stronger

warning when results have not been backed up.
**Recommendation.** I recommend that Hart investigate and determine if a software change could reasonably prevent this error in the future, and I request that they report their findings to us. This should have no effect on certification at this time.

## Conclusion

The Hart system is one of the best systems we have examined, and continues to improve. It should be certified with the conditions recommended.