

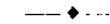


DEPARTMENT OF INFORMATION RESOURCES

P.O. Box 13564 ♦ Austin, TX 78711-3564 ♦ www.dir.state.tx.us
Tel: (512) 475-4700 ♦ Fax: (512) 475-4759

July 12, 2005

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



DIR BOARD OF
DIRECTORS



WILLIAM TRANSIER
Chair

LANCE K. BRUN

LARRY R.
LEIBROCK, Ph.D.

M. ADAM
MAHMOOD, Ph.D.

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 Hart Intercivic voting systems

Dear Ms. McGeehan:

I attended a scheduled re-examination on May 25, 2005, at 8:30 am, for the purpose of examining the voting system from Hart Intercivic. This report summarizes my findings.

Hardware/Software Version	Date Previously Certified
Ballot Origination Software System v4.1.0	June 24, 2004
Ballot now: Paper Ballots v3.0.24	June 24, 2004
eSlate v3.1.0	June 24, 2004
Judges Booth Controller v3.1.0	June 24, 2004
Tally, version v4.1.0	June 24, 2004
Rally, version v2.1.0	June 24, 2004
eCM Manager v1.0.7	N/A
SERVO v3.0.17	N/A
eScan v1.0.0	N/A

Collectively all these components are referred to as System 5.

New Focus on Security

Hart commissioned a complete risk assessment by an industry leader in digital security. From this assessment they developed a security plan and implemented it, resulting in numerous changes to all system components. The changes also meet new customer requirements and requests that were generated through Hart's work with another state.

Hart's system is now compliant with BS7799, which implements ISO 17799 (see <http://iso-17799.safemode.org/>). Hart is now audited quarterly to these standards. ISO 17799 is a code of practice for information security management. It contains 36 control objectives and suggests hundreds of specific controls, organized into 10 main sections. Each control objective contains advice on how to satisfy the objective, and includes a number of best practices for information security controls.

BS7799 is a specification for an Information Security Management System. The specification provides a system for monitoring, measuring and controlling information security as a whole. In effect it is a methodology for applying the controls contained in ISO 17799.

The vendor also noted that the audit log gets quite large for some jurisdictions. Thus in addition to the substantial changes to security methodology, they have provided a much improved searching and navigation engine with which to review the log. It is suggested that such facilities also be provided for the public to access and search the log.

eScan

The eScan is new to the Hart product line. It is a system hardware and software that scans and creates a digital image of the entire ballot. The software looks for patterns such as check boxes that it expects to find in specific locations on the ballot. It then determines if the voter has made marks in any of the boxes.

This approach produces a somewhat more stable, robust process than previous optical scan systems that scan only specific, limited areas of the ballot. In addition, the new scanner is not as sensitive to the kind of paper or pens that are used, compared to earlier technologies. The unit used for the demonstration was able to detect even tiny marks made by various pens and pencils in the selection boxes.

Voters insert ballots into the scanner. The scanner evaluates the ballot and accepts it or rejects it with instructions to the voter about the problems it encountered. However, the system provides no way for the voter or election officials to resolve errors electronically. The voter must change the ballot itself, or spoil the ballot and vote with a new one. The machine records all valid ballots as Cast Vote Records (CVR) but not as images.

When the polls close, the eScan can read the MBB from any DREs at the polling place, accumulate the totals of the DREs with the scanned paper ballots, and produce a precinct report. Thus if necessary, a small jurisdiction can still use paper ballots along with DREs, or use paper ballots in only part of the jurisdiction.

Note that the MBB is just used to collect CVRs and produce a precinct report. The report is not stored on the scanner or MBB. After the polls close, no device makes changes to the CVRs in the MBBs. The audit log in the scanner does record in the MBB the fact that the close-polls report has been created.

The vendor noted that they plan to eliminate the need for the JBC to reduce the cost per polling location. This may also increase the flexibility of their system, especially in cases in which a voting device malfunctions during the day and needs to be replaced.

BOSS

The most significant changes to BOSS revolve around Security. The MBB is now encrypted and uses SHA1 authentication. Boss now requires a hardware key to operate. This key is inserted in a USB port, and is unique for each jurisdiction. Further, each user must sign on using a user ID and password.

BOSS now provides enhanced support for separating party affiliation during primary elections. This feature improves reporting rather than voting, however, as the voters will see no changes to the way races are presented.

The vendor noted that the database is encrypted using the physical encryption key described earlier. There is no way to access the data without the physical key. Each major operation in the software requires user name and password. Such actions are recorded in the log, but not the serial number of the physical key that is used. The key is required only for Boss and Rally. More questions were asked of the vendor but were deferred to an executive session in which proprietary issues could be discussed.

Ballot Now

Ballot Now (see http://www.hartintercivic.com/files/ballot_now.pdf) prints ballots, scans cast ballots to record votes, notes anomalies such as overvotes and presents them to user for resolution. A few minor features were added to this product, as well as the security enhancements added to other products.

eScan

The eScan device is an optical scanner for use as a precinct tabulator as well as an early voting tabulator (see <http://www.hartintercivic.com/files/eScan.pdf>). Users insert ballots into the eScan, and the system checks the ballot for errors. Users are given a chance to retrieve ballots to correct the errors before casting them.

There were some questions about the version of eScan that was demonstrated. At boot-up, the version is displayed as 1.03 even though the version number given above for certification is 1.0. The vendor said this is because of engineering changes that were made at behest of ITA. The vendor said that there may be more changes, but likely shipped version will be called 1.0.

The EScan generated some discussion about a small utility the vendor uses internally to clear votes off of voting machines for testing and for demonstrations such as this examination. The existence of this utility creates a small chance that an unauthorized person with access to the program could cause a significant amount of mischief in a local jurisdiction. One of the examiners made a convincing argument that such a utility should at least require a password to use it.

Rally

Encrypted communication through Secure Socket Layer (SSL) has been added to remote data communication through Rally.

Servo

Apparently there is no way to transfer data to SERVO from eSCAN yet.

Results of the examination

The voting test did not uncover any anomalies in counting votes and the user interface.

The vendor's new initiative focusing on security is timely and seems well designed. However, there are some concerns about the new security devices and utility programs that should be addressed as soon as possible.

DIR finds no objections to certifying the system itself as presented at this examination.

Respectfully,

A handwritten signature in black ink that reads "Nick Osborn". The signature is written in a cursive style with a long horizontal line extending to the right.

Nick Osborn
Systems Analyst