# BALLOT NOW™

Intelligent Ballot Management

Hart InterCivic's Ballot Now System is a breakthrough product, combining state-of-the-art digital imaging and intelligent ballot management.


There are times when paper ballots are the best, or the only, alternative for conducting elections. For example, comprehensive election solutions must support absentee-by-mail or other special situations that may arise in modern elections.

Ballot Now offers paper ballots on demand, efficient processing of voted ballots, and unsurpassed efficiency when it is necessary to interpret voter intent. All of these features are included in a system that requires off-the-shelf computers, scanners and printers.

Ballot Now prints paper ballots on-demand for distribution to voters, either in person or by mail. Returned ballots are scanned and digital images are created for each ballot. Ballot Now captures each vote, creating electronic vote records that are then tabulated using the eSlate™ Electronic Voting System's powerful Tally™ tabulation and reporting application.system.

The Ballot Now Digital Ballot Imaging System can be a stand-alone paper voting system or fully integrated with the eSlate Electronic Voting System or another election system. Ballot Now comes complete with eSlate's Ballot Origination Software System™ for ballot generation and Tally tabulation software.

## ULTIMATE FLEXIBILITY IN BALLOT LAYOUT

Ballots need not be printed according to strict design standards required by typical proprietary optical scan systems. When formatting the ballots, Hart InterCivic's intuitive ballot generation software automatically matches the target zone for scanning to the area of the ballot to be marked by the voter. This eliminates human error in ballot formatting and the need for precise, costly printing. Security numbers may be printed on each ballot, preventing unauthorized ballot duplication or the same ballot being scanned twice. In addition, ballots can be printed on security paper to further reduce the possibility of fraud. Ballot Now creates ballots in multiple formats and prints on a variety of standard paper sizes and weights. Ballot Now also supports multiple languages.

## ON-SCREEN BALLOT RESOLUTION: A TRUE INNOVATION IN ELECTION MANAGEMENT

Voters sometimes mismark or unclearly mark ballots. In some states voter intent must be determined in these cases. In other states, voter intent is only analyzed in the case of a challenge or a recount. When it's time for election officials to review unresolved ballots in those cases where voter intent must be determined, Ballot Now presents digital images of each questionable ballot on the screen. Those contests requiring an interpretation of voter intent are automatically highlighted. Easy-to-use pull down menus offer election officials a range of choices for resolving ballot errors. When all ballot resolution determinations are made as necessary, Ballot Now creates an electronic cast vote record and adds it to the election results. Each resolution action is logged into Ballot Now's audit log, and there is no alteration of the original paper ballot. Ballot Now is the only paper ballot system on the market today offering optional on-screen resolution capability.

The eSlate voting booth's unique design makes it the ideal booth for voters, precinct officials, and elections office staff. In addition to offering a comfortable voting space for all voters, it is easy to store, transport, set up, and disassemble. The ballot is presented to all voters at an easy-to-view angle. The side, back and top panels assure every voter's privacy for casting a secret ballot.

### 6.04.02 Audit and Security

*a) How are summary reports of votes cast on each voting device created?*

Hart Response:

The System for Election Records and Verification of Operations (SERVO) software application provides an election records archiving and asset management system for the Hart Voting System. The SERVO application tracks the jurisdiction's Hart Voting System equipment and assists in archiving CVRs and managing election data. SERVO's primary purpose is to maintain ongoing equipment history and to manage election records as required.

SERVO is used to back up CVRs and audit logs from eSlate units and Judge's Booth Controllers (JBCs) and eScan units used in an election. The backed-up data can then be used to provide reports on CVRs, audit logs, and equipment used, and to provide recount data to Tally, if necessary.

SERVO is also used to recover data from equipment in the case of a lost or damaged MBB, and to reset equipment as needed. SERVO uses the triple redundancy features of the Hart Voting System to their fullest advantage. Election results are initially generated from the direct reading of MBBs into Tally. SERVO-generated recount data from the JBC and eSlate and eScan memories can also be compared to the MBB results. This process makes the ability to recount election results a seamless option for every election cycle, thereby increasing the confidence of election officials and voters.

SERVO is intended for use at a jurisdiction's warehouse, and is typically used before deploying the JBCs and eSlate and eScan units to the field and at the conclusion of an election. Equipment management tasks include adding a device's public serial number to the SERVO database and resetting a device.

SERVO produces the following standard reports:

- Equipment List
- Firmware History
- Connectivity
- Devices Backed Up
- Audit Search
- Device Audit Log
- Device Cast Vote Records
- Votes by Precinct
- SERVO Internal Audit

*e) How are data transferred from memory devices to a central host?*

**Hart Response:**

Voting results may be transferred from the polling place to any other location (after the polling place is closed) by simply removing the MBB from the JBC and eScan, and transporting it to the assigned location. Official results are obtained by reading the MBBs into the Tally tabulation software application.

*f) What safeguards are built into the voting system components to prevent tampering, theft or damage?*

**Hart Response:**

Hart is dedicated, as part of its commitment to election integrity and customer satisfaction, to the security of the information used in the product development process and to the security of the Hart Voting System, in which our customers and their voters place their trust.

Internally, the objective of information security is to prevent unauthorized access to and use of Hart information while allowing employees to fulfill their job responsibilities with as little hindrance as possible. Hart management implements information security to ensure contractual requirements are met, employees are trained in information security, and risks to information security are understood and minimized.

*Designed for Security*

Several key principles are at the foundation of the Hart Voting System's design:

- **Multiple Layers of Defense.** Security features should be established in a manner that requires an attacker to overcome multiple obstacles to reach a target. The Hart Voting System includes several key process areas where this is the case, for example, as the system's mulitiple original storage of cast vote records.
- **Segmentation.** The Hart Voting System was intentionally designed with multiple, individual components that are allowed to communicate with each other only when a need to do so arises. The approach provides distributed processing of data, with each component verifying and authenticating the output of the previous component. The distributed architecture establishes multiple, independent data paths through the system that are cross-verified throughout the election process.
- **Standalone Security.** Each component of the Hart Voting System is secure on its own, and not dependent on any other component for its security. Additionally, each component maintains its own audit logs, recording each transaction that occurs and noting errors or anomalies.
- **Encryption.** Hart has implemented cryptography in all functions of Hart's election software and election data exchange points. This additional and robust layer of 128-bit encryption provides a high level of data security throughout the election process.

Over the past several years, news reports have expressed concern about the use of smart cards to activate voting devices, and the possibility that a programmer could generate "homebrew" or counterfeit cards that would permit them to cast multiple votes. The Hart Voting System does not use smart cards or any programmable devices. Instead, the eSlate uses a four-digit Access Code printed on paper as the activation technique. The voter does not insert anything into the eSlate,

environment has three layers. Only users at the Election Administration layer can install hardware devices and control the logging of users' actions on the system. For all other users, actions are logged showing the action performed and the time/date of the action. Only the Global Administrator has the ability to turn off or edit this user access level.

The Election Administration layer allows the operator to have reasonably full use of the PC, but restricts the user from installing hardware; accessing, editing, or controlling the logging; and removing or altering certain important Windows 2000 files and Hart program executables. Only the Election Administrator may create new Restricted Users. The Restricted User layer allows no operating system access at all. The Restricted User may only operate the specified Hart Voting System application through the application interface at installation. Restricted Users may not view the file structure or access any operating system programs.

Further security measures include restricting network access at the BIOS level, and removing the "A" or floppy drive and "D" or CD drive from the boot chain. This measure removes the threat of attempting to connect the PC to a network, and the threat of anyone booting the computer to a floppy and thereby having access to the operating system. BIOS settings are secured with Administrator-level passwords.

Hart's eSlate Cryptographic Module (eCM) security device is required for access to secure functions in the BOSS, Ballot Now, Rally, Tally, and SERVO applications. In a given election, the signing key on the eCM device is used by the BOSS application to accept the ballot formats for the election, and a matching signing key must also be present in the eCM device(s) used in the Rally, Tally, and SERVO applications. For a given election, several eCM devices should be created in order to have a separate eCM device available for use with each computer running an Hart Voting System software application.

*Polling Place Security Features*
Before equipment is deployed to the polling locations, each JBC is pre-configured with an electronic signing "key." This key prevents the use of any Mobile Ballot Box (MBB) containing election data not generated with the same signing key.

At the polling place, the JBC's MBB compartment may be sealed with either a locking device or a security seal. Thus, any attempt to remove the MBB will require action that is easily detected. Booths may also be sealed with a locking device or seal when not in use, whether in storage or at a polling place.

The operating system for voting devices is a true embedded real-time system that is configured specifically for the intended election functions. Only the functions necessary to support the election operations are contained in the operating system, configured when the code is compiled. A real-time system has strict timing requirements such that any anomalous operation causes the system to generate a system error, halt operations, and notify the operator. Any external interference disrupts the timing and causes a system error. No access to the operating system exists; therefore, illegal operations are not possible.

Additionally, the use of proprietary firmware, database structures, and communication protocols provide security against tampering with any Hart Voting System component. The associated system fault warnings provide detection of such attempts.

Finally, because all actions taken on any Hart Voting System component, including voting hardware or ballot preparation and tabulation software, are audited, a record of intrusion activity will be included in the audit data.

*Physical Security*
Physical security is a key part of an overall security program both internally and externally. Hart emphasizes physical security for internal company processes and the Hart Voting System.

*Hart Corporate Security*
Internally, Hart has implemented thorough security measures to ensure the integrity of the Hart Voting System source code. For example, the server upon which source code rests has:

- A firewall to protect it from intrusion and virus files
- *Microsoft security templates enabled, including complex passwords changed* every 42 days, etc.
- Real-time antivirus scanning of all incoming files
- Real-time updating of virus definition files, which is then pushed to all computers on the network
- Daily full backup to prevent loss of any data

Hart also has instituted physical security measures for facilities management. Critical or sensitive business information processing facilities are housed in secure areas, protected by a defined security perimeter with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage, and interference. Access to all facilities is through card access. Confidential or proprietary information is locked in secure storage areas.

*Hart Voting System Security*
Hart recommends operating the Hart Voting System according to existing security procedures. All Hart elections warehouse facilities in the County should be locked with security and monitoring abilities. The PCs running election management applications should be kept in an access-controlled room, with the ability to lock the room when the system is not in use. Additionally, application PCs will not to be connected to any network, thus eliminating the opportunity for an external hacker to gain unauthorized entry.

At the polling place, the JBC's MBB compartment may be sealed with either a locking device or a security seal. Thus, any attempt to remove the MBB will require action that is easily detected. Booths may also be sealed with a locking device or seal when not in use, whether in storage or at a polling place.

*g) What are the reporting and audit techniques that are incorporated into each voting system?*

**Hart Response:**

included in the tabulation. The primary sorting order is by precinct name. The information includes the source of the ballots (absentee, Early Voting, Election Day), the total number of included provisional ballots in the precinct, and the total number of included provisional ballots in all precincts.

- **Ballot Status – Excluded – Retrievable** – lists which retrievable ballots are excluded in the tabulation. The primary sorting order is by precinct name. The information includes the source of the ballots (absentee, Early Voting, Election Day), the total number of excluded retrievable ballots in the precinct, and the total number of excluded retrievable ballots in all precincts.
- **Ballot Status – Included – Retrievable** – lists which retrievable ballots are included in the tabulation. The primary sorting order is by precinct name. The information includes the source of the ballots (absentee, Early Voting, Election Day), the total number of included retrievable ballots in the precinct, and the total number of included retrievable ballots in all precincts.
- **Blank Ballot Report** – lists the number of blank ballots cast, by precinct, during absentee, early, and Election Day voting. The primary sorting order is by precinct.
- **Canvass Report** – lists how each precinct voted for each candidate or choice in a contest, including number of absentee ballots cast in precinct, total number of ballots cast in precinct, and total number of votes cast in precinct for the contest
- **Cumulative Report** – provides voting results and summary totals for each contest in a jurisdiction. It also includes statistics by the number of precincts and by the number of votes for each contest, including number of absentee votes for the contest choice and total number of votes for the contest choice.
- **MBB Status Report** – provides information about MBBs defined in Tally. The report can be generated for either MBBs read by Tally (including identification of MBB, total number of MBBs read at the location, and total number of ballots read at the location) or MBBs that have not bee accounted for by Tally (including identification of the MBB that has not been read and the total number of MBBs that have not been read).
- **Polling Place Status** – lists the names of the polling places that have reported and the number of ballots cast at the polling place, the number of ballots cast in a polling place, the MBB identification(s) for the MBB(s) used in a polling place, and the number of MBBs used in a polling place.
- **Precinct Election Day Status** – lists the names of the precincts that have reported; number of registered votes in those precincts; the number of ballots cast in those precincts; and percent turnout in those precincts.
- **Precinct Election Day Status (with MBB IDs)** – used for precincts reporting or not reporting on Election Day. This report lists the names of the precincts that have reported; the number of registered voters in those precincts; the number of ballots cast in those precincts; and the percent turnout in those precincts.
- **Precinct Report** – lists results by precinct for every contest on a precinct's ballot, including number of absentee votes for the contest choice and total number of votes for the contest choice.
- **Precinct Turnout** – lists the voter turnout for the precincts in the election from the following vote sources: all voting (absentee, early and Election