Recent News Stories

Due to the interest and intensity of the upcoming November election cycle, there have been numerous stories in the media raising concerns about election security and voting methodologies. Hart has received many requests from customers asking for information in addressing questions on these topics. While, ultimately, it is up to local election officials to formulate their own statements, we are providing the following information to serve as useful background information:

- Regarding reporting on FBI investigations and DHS "alerts" related to election security, it is critical that our election administration clients, as well as the voting public, have compete information on the cyber-attacks that were not fully disclosed in the media.
- Readers may have been misled that voting equipment itself could be breached or their personal voting history or candidate vote selections may be subject to manipulation. This is not the case whatsoever.
- The suspected attacks (e.g. Arizona and Illinois) were on the states' voter registration systems (state-run lists of who is and who is not registered to vote) and not in any way related to the voting / tabulation systems (casting, capturing and counting of votes). Those are two completely separate systems and it is important that the public understand that distinction.
- Data breach attempts on voter registration systems, even if successful, cannot manipulate the way a vote is recorded for an individual voter. The way a person votes is NEVER connected to their individual voter record. The right to cast a private vote is sacred and a large part of why these two systems are kept completely separate.
- Hart InterCivic wholeheartedly supports and applauds the hard work being done by law enforcement and national security officials to detect potential gaps in voter registration system security, as well as the state election officials who are working to ensure the integrity of those systems.
- We also want to ensure the public understands that the security of the voting systems used to capture and tabulate their votes are NOT included within the scope of these recent stories.
- Hart InterCivic does not design or sell any products related to voter registration or related to the storage, maintenance or security of voter registration data. Our solutions are focused exclusively on the capturing and tabulation of votes and reporting and auditing of those results.

Hart's Approach To Security

- Hart voting systems, including all embedded security features, are rigorously tested and certified by the federal Election Assistance Commission (EAC) or its predecessor certification organization, the National Association of State Election Directors (NASED). In addition, many states require separate independent testing by state election authorities in order to receive state certification, and Hart systems have passed those state standards in the states where our systems are used.
- Security features of Hart voting systems include physical hardware access controls and multi-factor authentication on software. Audit features allow election officials to maintain and access a detailed electronic record of all activities that occur related to system software, as well as the ability to review anonymous cast vote records to verify that the system software tabulates properly.
- None of Hart's voting systems are connected to the internet or wireless networks, nor are they even connected to an office network or intranet.
- External cards, drives or other devices can NOT be inserted by voters into any Hart voting device, nor can executable code be hidden and run from voting system media cards.
- Strong chain of custody processes within jurisdictions prevent data manipulation as it is being transferred from the voting devices to a central count facility. Multiple redundant data backups ensure any such manipulations would be detected.
- Cast vote record data is digitally signed using NIST-compliant FIPS 140-2 cryptographic modules.
- Hart voting and election solutions are in NO way connected to any of the following:
    - Internet
    - Intranet or in-office networks
    - Voter rolls/registration
    - Voter personal data
    - Campaign/donor information
    - Party/campaign volunteer information or schedules
    - Voter communications regarding times/locations for early or Election Day voting
    - Email systems
- Digitally-signed data, stored redundantly in multiple places provides clear, reliable audit results, for all of our voting solutions, be they paper ballots or direct record electronic ballots.
- All election system solutions from Hart deliver best-of-breed security, auditability, performance and reliability...resulting in smooth-running elections and complete confidence in the election results.

HVS Security & Auditability Feature Highlights

For those jurisdictions using the Hart Voting System, election officials and voters benefit from specific features designed to deliver high performance and reliable security, resulting in a high degree of confidence:

- The Hart Voting System includes both physical and electronic intrusion detection controls, such as standard election seals and time-stamped transaction logs that record every system action related to the voting process.
- The Hart Voting System provides:
    - Digital encryption to protect data.
    - Multiple memory storage of cast ballot data.
    - Self-contained components that are not externally networked.
    - Thorough audit logs that provide transparency.
    - Malicious code, or any executable software, cannot be run off of the data card from the polling place. The technology simply doesn't support this scenario.
- eSlate
    - Once a vote is cast on the eSlate system, multiple copies of the electronic ballot are saved simultaneously in different locations (on the eSlate, on the JBC and on the MBB which is inserted in the JBC), making lost data or undetectable fraud virtually impossible.
    - The eSlate's SELECT Wheel™ interface does not require calibration like older touch screen systems. There is no chance of false touches due to ballot images that are misaligned with touch sensors.
    - The eSlate has no external openings that could create a breach in the system's security that might provide access for creative hackers or others seeking to tamper, subvert, or vandalize the system or the election.
    - The system's eSlate® device allows the voter to double-check the ballot before casting it.
    - Each of the vote records can be verified and audited for security and accuracy.
- eScan
    - The eScan provides triple redundancy of the voter's choices: on the MBB flash memory card, within the eScan memory, and on the original marked paper ballot.
    - The scanned paper ballots are secured in a locked ballot box connected to the eScan.
    - The eScan also provides an electronic audit log that records all actions performed on the device with a date-time stamp.
    - The audit log can be printed out as needed by the jurisdiction.