Statement on Security & Auditability

Introduction

This document is designed to assist Hart customers by providing key facts and support in preparation for the upcoming November 2016 election cycle. It is divided into five distinct sections:

Page 1: Introduction & Background

Page 2: Recent Media Stories

Page 3: Hart's Approach to Security & Auditability

Page 4: Hart Voting System (HVS) Security & Auditability Feature Highlights

Page 5: Verity Security & Auditability Feature Highlights

Background

In preparation for the upcoming high-profile November Presidential Election, Hart InterCivic is working with customers to ensure they are ready for smooth election processes. Our proactive communication includes helping customers to understand and answer questions about such things as the security and auditability of their voting systems.

Much of this confidence Hart customers have in their voting systems is driven by Hart's approach to the critical areas of Security and Auditability:

- The Hart Voting System and the Verity Voting system are regulated, tested and certified at both the federal and state levels. The nearly 100,000 devices Hart has in the field have both been proven to be secure and accurate, successfully capturing and reporting millions and millions of votes across nearly 600 jurisdictions representing over 26 thousand precincts and nearly 30 million registered voters.
- Symantec, an acknowledged leader in technology security, has independently audited the Hart Voting System to ensure the highest quality of accuracy.
- Security comes not only from hardware/software technology features, but also from the people who use the systems and the procedures they follow. Hart encourages jurisdictions to utilize best practices to mitigate risks. Some include:
    - Employing a chain of custody processes, physical numbered and logged security seals on devices, no access to the internet or intranet and experienced trusted election administrators on staff
    - Conducting Acceptance Testing upon receipt of equipment
    - Election Logic and Accuracy Testing of the database for each specific election (conduct as provided under your respective State law)
    - Post- Election reconciliation of results and auditing

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.

Verity Security & Auditability Highlights

Those Hart customers ready for a modern upgrade have the benefit of being able to choose Hart's newest federally certified voting system: Verity. Verity is built on the same philosophical beliefs that has defined Hart for decades, including: innovation, security, accessibility and transparency. However, Verity also incorporates the very latest technology, as well as all the learnings from years of providing successful solutions to the elections community. Verity's unique features include:

- Throughout all phases of operation, all Verity system components maintain complete audit logs.
- Every Verity application thoroughly logs all user authorization/authentication, data entry, user interaction, and system events.
- Election managers can print or export audit logs from each application, using easy-to-use report filtering to access the precise information to be audited.
- Hardware
    - Verity's hardware physical features prevent physical tampering.
    - The access controls include keyed locks, features to support the use of tamper-evident seals, port protection, non-standard electrical wiring in strategic areas, and a two-factor authentication device used to secure access to critical functions throughout the election.
    - All ports on Verity voting devices are physically shaped in non-standard ways and accommodate only Hart-proprietary cables and devices in order to prevent unauthorized users from inserting standard, commercial-off-the-shelf cables or devices into Verity voting machines.
    - On the Verity Touch Writer and Verity Touch voting devices, audit logs and cast vote records are redundantly stored to the vDrive and to a partition on the internal compact flash card. The audit log for each device includes a record of each event occurring on the device.
- Software
    - Verity's software security mechanisms prevent modification of internal configurations at all times.
    - All Verity Voting software applications are installed in a secure "kiosk" mode that disallows user access to the operating system of the workstation on which the application is installed.
    - Voting data is digitally signed, which provides the same tamper-evidence as encryption while still allowing users to manually view and audit the data outside of our system.
    - Verity Software's audit log includes the Verity user's login ID and a record of all resolution decisions, providing a complete record of the adjudication process.
    - Hart offers a software tool that can be used in conjunction with, and as a supplement to, polling place reporting of precinct results and as an additional consolidation and auditing tool.