



## Electronic Voting Machine Information Sheet

### Avante Vote-Trakker

**Name / Model:** Vote-Trakker / EVC-308SPR<sup>1</sup>  
**Vendor:** Avante International Technology, Inc.  
**Voter-Verifiable Paper Record Capability:** Yes.



#### **Brief Description:**

Avante's Vote-Trakker 1 (EVC-308), was the first system to deliver a voter-verified paper audit trail. The Vote-Trakker 2 (EVC-308SPR) is Avante's latest voting machine with this capability. Voters use a "smart card" called a Voter Identification (VID) card to initialize the machine. After voting, the voter inspects a paper printout of their vote behind clear plastic. The voter then either cancels the vote or approves it. When cast, the paper record of the vote is deposited into an attached ballot box and the electronic record of the vote is written to flash memory and a hard drive within the machine. At the end of the election, the contents of the hard-drive are written to a writeable CD-ROM. Finally, the attached ballot box and the CD-ROM are transported to a tabulation facility where the CD-ROMs from all precincts are read into a central tabulation computer and summed to produce an aggregate vote count. This system is used only in Warren County, NJ.

**Detailed Voting Process:** After confirming the voter is registered, he or she is handed a "smart card" called a Voter Identification (VID) card to activate the voting machine.<sup>2</sup> This allows the machine to vote once. A "smart-card" is a card the size and shape of a

<sup>1</sup> See: <http://www.vote-trakker.com/overview.html>

<sup>2</sup> Note that Avante uses what is called a "contactless," "non-directional" smart card. Respectively, this means that the chip inside the card is not exposed and it does not matter which way the card is inserted into the machine. These types of smart cards are more difficult to hack and easier for voters to use.



## Electronic Voting Machine Information Sheet

credit-card which contains a computer chip, some memory and basic data such as the voter's ballot style.<sup>3</sup>

After using the touchscreen to vote, the SPR can then print a paper record. Displayed under clear plastic to avoid manipulation (see ballot box to the left of the machine in images above). The voter inspects the printout for accuracy. If the vote is incorrect, the voter indicates as so using the touchscreen and is given another chance to fix their mistakes after the paper record is deposited in a compartment in the machine for spoiled votes. If the vote is correct, the voter indicates so using the touchscreen and the machine prints a barcode on the paper record and drops it into the ballot box attached to the machine.<sup>4</sup> At the same time, the vote is electronically recorded internally to flash memory and an internal hard drive as ballot images.

At the end of the day, a poll worker with a special poll worker card closes each machine. The contents of the hard drives in each machine<sup>5</sup> are then written to a writeable CD-ROM (also called a CDR). The CDR can only be written once and cannot be changed afterwards. The CDR with the vote data and ballot box for each machine is delivered to a tabulation facility. At the tabulation facility, the vote data is read off of the CDRs from each precinct and fed into Avante's tabulation software. What is done with the paper audit records varies highly by state and county.

### What to Look For

- **Security Seals.** Ideally, the Vote-Trakker's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **The Memory Card is Sensitive.** Corrupt memory cards can introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.

---

<sup>3</sup> The ballot style specifies the races in an election and can be specific to a precinct and, during a partisan primary, the voter's political party. The card contains a 24 character randomly generated number that is used to connect the electronic ballot with the paper record.

<sup>4</sup> The barcode facilitates efficient counting of the paper records and contains no information about the voter.

<sup>5</sup> Note that if a question arises about the integrity of a CDR or hard-drive in case of a discrepancy between the paper records and the CDRs, the internal flash memory can serve as another redundant check. This is a last resort as it involves opening the Vote-Trakker's case.



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

### Past Problems:

None known.

**05/20/04:** Vote-Trakker EVC-308SPR Touch Screen DRE (firmware 4.7.6)<sup>6</sup>

### References:

The information in this document was obtained from David Alampi at Avante International Technology, Inc.

---

<sup>6</sup> The SPR is fully NASED-qualified against the Federal Election System's 2002 Voting System Standards.



## Electronic Voting Machine Information Sheet

### Advanced Voting Solutions WINVote

**Name / Model:** WINVote<sup>7</sup>

**Vendor:** Advanced Voting Solutions

**Voter-Verified Paper Record Capability:** None



**Brief Description:** The WINVOTE is a tablet-like touch-screen voting terminal equipped with a wireless local area network (LAN), a 15" full color screen with ZOOM capabilities, and built-in battery backup power, modem, and printer. When operational in a live election environment, the WINvote terminal rests in a plastic voting booth/secretcy and transportation case. It is designed as a stand-alone system to function both as a traditional precinct voting device and as a non-geographic voting station. This system is used in Hinds County, MS and 32 jurisdictions in VA.

**Detailed Voting Process:** After checking in at the polling place, the voter will approach one of the terminals. An election official will activate the machine. The voter will touch the "Click Here to Start" button on the welcome screen, and the ballot-marking process will begin.

The screen will display one race at a time, with available choices listed below the race name. Write-in candidates can be selected by touching the "Write-In" button at the bottom of the choice list. After making a selection, touch the "Next" button on the bottom of the screen.

When all selections have been made, the voter will be taken to a summary screen that lists that name of each race and the option that was selected by the voter. If the voter wishes to change any of these races, he/she should simply touch the name of the race and make another selection.

When the voter is satisfied with the summary screen, he/she should touch the red "Next" button on the bottom-right part of the screen. The next screen has a large red "VOTE" button. After touching that button, the ballot has been cast.

### **What to Look For**

- Security Seals. Ideally, the WINVote's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The

---

<sup>7</sup> <http://www.advancedvoting.com/index.php?p=votingequipment>



## Electronic Voting Machine Information Sheet

integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this:

<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- The Memory Card is Sensitive. Corrupt memory cards can introduce viruses, cause the main election server to crash and falsify votes. Access to the MBB memory card should be controlled, monitored and logged at all times.
- Wireless Vulnerabilities. The WINVote can be used in a wireless mode that involves individual machines talking to a controller in each precinct as well as machines and this polling place controller talking to a central election management system.<sup>8</sup> Wireless transmission of voter authentication and vote data can be very problematic and prone to error and malicious intervention. Moreover, there is evidence that the WINVote system operates over cellular frequencies (CDPD) as well as wireless data frequencies (802.11b) which considerably widens the possibilities of remote tampering.

### Past Problems

**May 2005:** *Mississippi*. Batteries failed early in the election, taking down the machines.<sup>9</sup>

**November 2003:** *Virginia*. The software failed (machines crashed throughout, voters reported difficulty in getting their choices to record), the hardware failed (some machines required new batteries, some needed to be “jiggled” back into operation, modems failed to transmit data).<sup>10</sup>

**November 2003:** *Mississippi*. Voting computers at some polling places in District 29 failed to start up. Others overheated and broke down during the election, and not enough paper ballots were available to allow all voters to vote.<sup>11</sup>

**06/17/02:** Firmware 1.54

### References:

VerifiedVoting.org, <http://verifiedvoting.org/article.php?id=5138>

---

<sup>8</sup> Eric C. Griffith. (2003, May 23). 802.11 at the Polls. Internet.com. Retrieved October 29, 2008, from [http://articles.directory.net/802\\_11\\_at\\_the\\_Polls\\_-a882441.html](http://articles.directory.net/802_11_at_the_Polls_-a882441.html) .

<sup>9</sup> Pearl turnout reported low; problems mar voting in Jackson's Precinct 36. The Clarion-Ledger. May 3, 2005. By Cathy Hayden. <http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20050503/NEWS0103/50503011>

<sup>10</sup> Operation Ballot Integrity. A Report by Fairfax County Republican Committee. January, 2004. [http://www.fairfaxco-gop.org/download/ballot\\_integrity.pdf](http://www.fairfaxco-gop.org/download/ballot_integrity.pdf)

<sup>11</sup> Long lines, machine malfunctions mark today's voting. November 4, 2003; By Clay Harden. <http://www.clarionledger.com/news/0311/04/mvproblems.html>



## Electronic Voting Machine Information Sheet

### Danaher/Guardian ELECTronic 1242

**Name / Model:** ELECTronic / 1242<sup>12</sup> (also known as the Shouptronic)

**Vendor:** Guardian Voting Systems, Inc. (division of Danaher Controls, Inc.)

**Voter-Verifiable Paper Record Capability:** None



**Brief Description:** The Guardian Voting Systems ELECTronic 1242 is a poll worker-activated full-face direct recording electronic voting system. Voters press the front of a mounted ballot (see rightmost image above) underneath which a touch-sensitive matrix of switches records choices. Poll workers activate the machine using an operator panel on the back of the machine to choose the ballot style and voters make choices by touching a numbered box next to their choice. When cast, voting records are recorded internally to eight memory locations: three banks of battery-powered RAM,<sup>13</sup> three banks of EEPROM<sup>14</sup> memory, one bank of EPROM<sup>15</sup> memory and a removable memory cartridge, which contains both EPROM and EEPROM memory. When polls are closed, poll workers remove the memory cartridge that contains the vote records from each machine. These cartridges are then either physically transported to a tabulation facility or their contents transmitted over modem using a cartridge reading device. This system is used in AR, DE, KY and PA.

**Detailed Voting Process:** When voters enter the precinct, poll workers confirm that they are properly registered to vote. The poll worker uses an operator's panel on the back of the machine to choose the ballot style appropriate for that voter.<sup>16</sup> The voter enters the curtains (see pictures at left above) and only the races for which they are permitted to vote are activated. The voter then votes by pressing a numbered box beside each choice

<sup>12</sup> <http://guardianvoting.com/gvs/vs.html>, accessed on October 26, 2006.

<sup>13</sup> This Random Access Memory (RAM) is similar to the memory that is used in a typical personal computer where a constant supply of power is necessary to keep data in memory. However, a 10-year life, lithium battery cell provides constant power to the ELECTronic 1242's RAM.

<sup>14</sup> EEPROM is electrically erasable, programmable read-only memory and retains data when un-powered.

<sup>15</sup> EPROM is erasable, programmable read-only memory and can only be erased with ultraviolet light.

<sup>16</sup> There may be different races for different precincts or political parties in one polling place.



## Electronic Voting Machine Information Sheet

in each race on the ballot. Flashing lights on the left-hand side of the ballot indicate races for which the voter has not yet voted. If the voter tries to choose more than one choice in a given race (over-voting), the machine will ignore the second choice. If the voter makes a mistake, they can press the numbered box again to deselect their choice; the indicator light will go out. The voter may then select the correct choice.

When done voting, the voter presses a large green “Vote” button in the lower-right corner of the voting machine. It is very important that the voter does not push the vote-casting button until they are done voting; a vote inadvertently cast may not be redone. Once cast, the vote is recorded internally to eight internal memory locations: three banks of battery-powered RAM that reside on the machine’s central processor, two internal banks of EEPROM memory, one bank of EPROM memory and a removable memory cartridge, which contains one bank of EPROM and one bank of EEPROM memory. The vote records are stored in “vote tables” as aggregate vote tallies and also as ballot images both internally and to the removable memory cartridge.

When the polls close, the machines print out paper copies of the results and poll workers remove their memory cartridges, which contain the vote records from each machine. At this point, the cartridges are physically transported to a tabulation facility. At the tabulation facility, election officials use a cartridge reader to read the data off of the cartridges and into vote tabulation databases. The results are then combined to produce an aggregate vote tally. The printed total tapes and memory cartridges can then become part of the official record of the election.<sup>17</sup>

### What to Look For

- Security Seals. Ideally, the 1242’s exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this:  
<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- Memory Cards. The 1242 is an older type of machine that uses a particularly sensitive and volatile type of memory (battery-backed RAM memory). Care should be taken with memory cards and they should only be handled by poll workers and authorized election officials, then in controlled circumstances such as the opening and closing of polls.
- Broken buttons, broken lights. The 1242 is a “button-matrix” DRE where the voter presses a button over which the machine’s paper ballot face is placed (under a plastic cover). A light lights up next to each selection by the voter. These

---

<sup>17</sup> Ballot images can be re-read off of the redundant memory inside the machine if a cartridge fails.



## Electronic Voting Machine Information Sheet

buttons and lights, especially the frequently used ones in Federal races, can break or burn-out. If you see evidence of this – e.g., a light not lighting up after multiple button presses – you should request that the machine be pulled from service or that the button in question be serviced.

- Fleeing voters/premature voting. Some voters can be easily confused in that they press the large “VOTE” button too early or not at all. If a voter complains that they only were able to vote on the first few races, they probably pressed the “VOTE” button before they were finished voting their ballot. Unfortunately, there’s not much to be done here other than emphasize that voters should make sure that they press the “VOTE” button *only after* they are certain they have voted as they want to in all races on the ballot. If a voter neglects to press the “VOTE” button and leaves a valid ballot on the machine, poll workers will probably have procedures to deal with this problem. We recommend that a poll worker reach in between the curtains and simply cast this vote.
- Incorrect ballot style. The 1242 can accommodate a number of different ballots, for different precincts, by disallowing voters to vote in contests for which they are not eligible. If a voter complains that their party (in a primary) races are not activated or that local races specific to their precinct are not activated, the poll worker probably pushed the incorrect ballot style option. The poll worker should cancel that ballot and activate the correct one.

## Past Problems

**April 2008:** *Pennsylvania:* Danaher Shouptronic in Bucks, Delaware, and Philadelphia County malfunction, causing long lines at the polls.<sup>18,19,20</sup>

**May 2007:** Reports of Shouptronic malfunctions in Philadelphia.<sup>21</sup>

**May 2005:** *Pennsylvania:* Votes were lost on the Danaher 1242 Shouptronic paperless voting machines. Since the number of lost votes could affect the outcome of three races, the 199 people whose votes were lost may be asked to revote.<sup>22</sup>

---

<sup>18</sup>“Downed voting machines caused delays in Falls.” Phillyburbs.com, April 22, 2008, available at: <http://www.votersunite.org/article.asp?id=7650>

<sup>19</sup>“Machines malfunction.” Philly.com, April 22, 2008, available at: <http://www.votersunite.org/article.asp?id=7647>

<sup>20</sup>“More voting machine malfunctions.” Philly.com, April 22, 2008, available at: <http://www.votersunite.org/article.asp?id=7646>

<sup>21</sup>“Problems at the polls.” ABC 6 Action News. May 15, 2007, available at: <http://abclocal.go.com/wpvi/story?section=news/politics&id=5305908>

<sup>22</sup> Berks County may ask people to vote again in two precincts. CentreDaily.com. May 18, 2005. Associated Press. <http://www.centredaily.com/mld/centredaily/news/politics/11680418.htm>. Archive at <http://www.votersunite.org/article.asp?id=5408>



## Electronic Voting Machine Information Sheet

**November 2004:** *Ohio.* Phantom votes appear in the presidential totals. Bush received 4,258 votes and Kerry received 260 in a precinct with only 638 voters.<sup>23</sup>

**November 2003:** *Tennessee.* A poll worker in Rutherford County inadvertently cast a vote during a demonstration that may have resulted in a tie for a Town Council position.<sup>24</sup>

**October 2001:** *Tennessee.* In Knox County, a voting machine showed an error code that corresponded to a discrepancy between internally stored vote tables. Local officials could not retrieve the data or have the machine print out the results. A Danaher technician was able to crosscheck the internal memory tables and provide results.<sup>25</sup>

**November 2000:** *Tennessee.* About 7% of memory cartridges in Knox County were temporarily unreadable and three cartridges remained unreadable. There were also problems with transmitting precinct-by-precinct vote totals.<sup>26</sup>

### References

The Philadelphia City Commissioners Office. "Risk Assessment of Danaher Controls DRE Electronic [1242] Voting System and Philadelphia Procedures." Prepared by: Bob Lee, Voter Registration Administrator (March 9, 2004).  
[http://josephhall.org/misc/danaher\\_1242\\_philly\\_report.pdf](http://josephhall.org/misc/danaher_1242_philly_report.pdf)

The Department of Elections for New Castle County. "Report of the Committee to Review Physical and Operational Security of the Danaher Controls 1242 Electronic Voting Machine." (June 22, 2004). [http://josephhall.org/misc/Delaware\\_VM\\_Report.pdf](http://josephhall.org/misc/Delaware_VM_Report.pdf)

---

<sup>23</sup> Computer error at voting machine gives Bush 3,893 extra votes. Akron Beacon Journal. November 5, 2004. Associated Press. <http://www.ohio.com/mld/beaconjournal/news/state/10103910.htm?1c>

<sup>24</sup> "Mistaken vote may have led to Smyrna election tie." Associated Press State & Local Wire, November 19, 2003.

<sup>25</sup> "City Council Primary Election Results Certified; Accurate Ballot Count Finally Obtained From Malfunctioning Machine." Knoxville News-Sentinel (Tennessee), October 7, 2001.

<sup>26</sup> "Report on voting difficulties due within a week; Voters get chance to detail problems." Knoxville News-Sentinel (Tennessee), November 14, 2000.



## Electronic Voting Machine Information Sheet

### ES&S AutoMARK Voter Assistance Terminal

**Name / Model:** AutoMARK VAT <sup>27</sup>  
**Vendor:** Election Systems & Software  
**Voter-Verified Paper Record Capability:** Yes.



**Brief Description:** The AutoMARK VAT uses a touch screen interface with optical scan paper ballots. It is used in ~30 states. The AutoMARK VAT is an optical scan ballot marker designed for use by people who are unable to personally mark an optical scan ballot due to physical impairments or language barriers. Accessibility features include a touch screen with a zoom and contrast feature, multiple language translation, keypad marked with Braille, puff-sip interface as well as an audio ballot feature. The AutoMARK VAT prevents over-voting and users are prompted visually and audibly if they attempt to under-vote. Under-voting is allowed only after the user is prompted unless otherwise required by the election jurisdiction. Before any mark is made on the ballot, the voter is shown a verification screen where each race is displayed along with their selections. Under-voted races are clearly identified by different colors on the touch screen as well as the audio ballot prompt. The AutoMARK VAT marks the optical scan ballot for the voter including any write-ins. For voter verification purposes, the user may also re-insert their marked ballot in order to verify that their intent was accurately captured. In the event of a mis-marked ballot the voter may spoil the ballot, obtain a new ballot and restart the voting process.

**Detailed Voting Process:** The AutoMARK™ Voter Assist Terminal (VAT) is a hybrid of several devices: a scanner, printer, touch screen display, and input device. The data for

---

<sup>27</sup> See <http://www.automarkts.com/>



## Electronic Voting Machine Information Sheet

a given election is stored on a compact flash card. Using Automark Technical Systems proprietary software, an election official is able to convert election data created using industry standard software for use in the AutoMARK VAT. During this process it is also possible to customize the election data, including adding translations or phonetic pronunciation of difficult names for use with the synthesized speech. Once the flash card has been programmed, it is inserted and locked into the AutoMARK VAT. Secure electioneering is verified by a special program that fills in each oval on a ballot along with the candidate's name.

When a voter inserts their ballot into the AutoMARK VAT, it searches for a match to the precinct identification code found on each ballot and used by industry standard optical scanning devices. The voter is then prompted to select the language in which they wish to vote and is able to carry out the voting process using the touch screen, a puff-sip device, or by following audio prompts along with a keypad. Additionally, there is a screen privacy option voter so that visually impaired users can be assured that their voting remains private. During the voting process, over-voting is not allowed. The user is also prompted anytime they attempt to under-vote, and may select to continue with the under-vote or re-vote the contest in order to properly capture their intentions. Before any mark is made on the ballot, the user is shown a verification screen where each race is displayed along with the users' selections. Under-voted races are clearly identified and the user is given the option to return and modify any race they choose.

The ballot is then printed, along with any write-ins, and returned to the user. For voter verification purposes, the user may also re-insert their ballot, after printing is complete, in order to verify that their intent was captured. If not, they may simply follow jurisdiction-specific ballot spoiling procedures and restart the voting process.

### What to Look Out For

- **Security Seals.** Ideally, the AutoMARK's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **System Crashing.** The AutoMARK can often crash when the ballot is being inserted and read and results in the system hanging with the inserted ballot stuck in the feed bath. Poll workers should reboot crashed machines and perform the "Eject Ballot" operation.
- **Boot-up Times.** The AutoMARK, especially the A100 model, can take up to 15-20 minutes to reboot. If rebooting happens often, this can severely affect voters who require the AutoMARK to cast a ballot.



## Electronic Voting Machine Information Sheet

- “Ballot Not Recognized” or “Ballot Misfeed” Errors. In California State testing,<sup>28</sup> 6-8% of the time the blank ballot inserted into the AutoMARK by a would-be voter was not recognized by the machine. Usually, in the California testing re-inserting the ballot would not reproduce this error. When the voter inserts a blank ballot with a slight skew, so that it’s not aligned properly, the AutoMARK may return the ballot and report a “Ballot Misfeed” error. Re-inserting the ballot should work to allow the ballot to be read.
- Ballot Damaged. Occasionally, the AutoMARK will severely damage a ballot when it ejects the ballot. Most often, this results in a ballot that cannot be fed into the corresponding optical scan reader. The ballot should be reissued and the voter should go through the AutoMARK marking process again.

### Past Problems

**November 2008:** *Wisconsin.* When a blind voter tried to use the AutoMARK unit in early voting, it displayed an error code; when that was cleared the device failed to print her ballot because it was “out of ink.”<sup>29</sup>

### References:

ES&S Unity 3.0.1.1 Source Code Review for California Secretary of State Office of Voting Systems Technology Assessment, February 15, 2008

[http://www.sos.ca.gov/elections/voting\\_systems/unity\\_3011\\_source\\_code.pdf](http://www.sos.ca.gov/elections/voting_systems/unity_3011_source_code.pdf)

“Limited-Scope User Acceptance Test Results of the AutoMARK™ Vote Assist Terminal” in Wake County, InfoSENTRY, April 25, 2006

[http://www.ncvoter.net/downloads/WakeInfoSENTRY\\_AutoMARK-UAT\\_Report\\_20060425.pdf](http://www.ncvoter.net/downloads/WakeInfoSENTRY_AutoMARK-UAT_Report_20060425.pdf)

---

<sup>28</sup> [http://www.sos.ca.gov/elections/voting\\_systems/unity\\_3011\\_volume\\_test.pdf](http://www.sos.ca.gov/elections/voting_systems/unity_3011_volume_test.pdf)

<sup>29</sup> See [http://www.wkowntv.com/Global/story.asp?S=9255798&nav=menu1362\\_2](http://www.wkowntv.com/Global/story.asp?S=9255798&nav=menu1362_2)



**Electronic Voting Machine Information Sheet**  
**ES&S DS200 Digital Scan System**

**Name/Model:** ES&S DS200 Digital Scan System

**Maker:** Election Systems & Software

**Voter-Verifiable Paper Trail Capability:** Uses paper ballots



**Brief Description:** The ES&S DS200 is a precinct-based, voter-activated paper ballot counter and vote tabulator. The DS200 possesses a 12" LCD touch screen, which is used to provide voters with feedback, such as an overvote warning. When the polls close, the ES&S DS200 prints out the voter logs so election officials can have a paper tally.<sup>30</sup>

**Detailed Voting Process:** The ES&S DS200 functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter then shades in the paper ballot with any standard pen or pencil and inserts the ballot into the ES&S DS200, where they are given a chance to review their votes. As votes are entered, the ES&S DS200 stores the vote tallies on its internal memory card. Optional land line and wireless modems are available for the DS200.<sup>31</sup> When the polls close, the ES&S DS200's internal printer prints out the precinct's vote report on paper.<sup>32</sup>

---

<sup>30</sup> From the manufacturer's product brochure, available at:  
[http://www.essvote.com/HTML/docs/brochure\\_DS200\\_US\\_v5.pdf](http://www.essvote.com/HTML/docs/brochure_DS200_US_v5.pdf)

<sup>31</sup> Id.

<sup>32</sup> Id.



## Electronic Voting Machine Information Sheet

### What to Look For

- **Security Seals.** Ideally, the DS200's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should locked and/or be sealed with tamper-evident tape.
- **The Memory Card is Sensitive.** Corrupt memory cards may be able introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, black ballpoint pen that does not bleed through paper.

### Past Problems:

**August, 2008. Florida.** In two counties, problems with DS200 scanners were noted; in Pinellas, screens froze and there were paper jams. In Pasco, minor problems occurred, followed by the inability to transmit results by modem.<sup>33</sup>



## Electronic Voting Machine Information Sheet

### ES&S iVotronic

**Name / Model:** iVotronic<sub>1</sub>

**Vendor:** Election Systems & Software, Inc. (ES&S)

**Voter-Verifiable Paper Trail Capability:** Yes



**Brief Description:** ES&S' iVotronic Touch Screen Voting System is a touch screen voting machine that records votes on internal flash memory. A poll worker uses a device called a Personal Electronic Ballot (PEB; pictured above at left) to turn the machine on and enable voting. Voters choose their ballot language and then make their selections using a touch screen, much in the same way that modern ATMs work. When the polls close, poll workers move summary data from each machine onto the PEB. The PEBs are then transported to election headquarters or their contents transmitted via a computer network.

**Checking the Voter-Verifiable Paper Trail:** The iVotronic has an optional voter-verifiable paper trail printer, known as the Real-Time Audit Log (RTAL). States such as Ohio, West Virginia, and North Carolina require the RTAL by law, while iVotronics in South Carolina, Texas, and Pennsylvania do not have this option. The RTAL printer is a reel-to-reel cash-register type of printer under transparent plastic, and is located just to the left of the touch screen (pictured above right). The RTAL records all of the voter's actions, so if a voter changes her mind about a race on the ballot, the RTAL records both the initial choice and the final choice.

**In Detail:** When the voter enters the polling place, a poll worker first confirms the voter is registered. Then the poll worker walks with the voter to an iVotronic and inserts the PEB in the PEB slot (visible as the rectangular slot in the upper left corner of the middle image above). The PEB communicates with the iVotronic using infrared signals, much like a TV remote control works, except that the PEB and iVotronic will not communicate unless the PEB is completely inserted. If the election requires a party-specific ballot, the



## Electronic Voting Machine Information Sheet

poll worker chooses this for the voter. Activation by the PEB enables the iVotronic to vote once.

The voter then selects a ballot language and makes decisions using the touchscreen. When the voter is done, he or she presses a small “vote” button at the very top of the iVotronic to cast the vote. The vote is then recorded to three internal flash memories that reside inside the machine. A fourth memory is a removable card, called a “compact flash” (CF) card; note that CF is the same technology used in many digital cameras to store photos. During the election, the CF card holds audio files (for those with visual disabilities) and ballot definitions; vote data is written to the CF card when the machine is closed.

A poll worker closes the polls by using the PEB with a password to enter a supervisor menu on each iVotronic. After closing the election for a given machine, summary vote data are transmitted to the PEB via infrared signals.<sup>34</sup> After the PEB is used to close all the iVotronic machines, it contains all the summary data for the precinct. Depending on local regulations and procedures, poll workers can use a “printer kit” at this point to print the result summary from the PEB on to paper. The PEB for that precinct, any printouts and the CF cards are then either physically transported to a central tabulation facility or its contents sent over a computer network using a laptop running ES&S' Unity software.

### Things to Look Out For

- The PEB slot on the face of the iVotronic is particularly sensitive. The EVEREST study showed that a voter with a magnet and a properly programmed PDA (with an infrared port) could gain privileged access to the sensitive functions of the machine. If you see anyone spending a long time in an iVotronic voting booth and engaging in activity that appears to be centered around the upper-left part of the iVotronic, they might be messing with the PEB slot. Of course, they might also just be voting, so don't cry wolf.
- The VVPAT printer (RTAL printer) is connected to the iVotronic via a cable that is connected to the top of the machine. This cable, unless the jurisdiction has purchased special cables or connectors, can be disconnected by a voter and various types of mischief could be performed (from printing extra VVPAT records to messing with the internals of the iVotronic). If you observe anyone disconnecting this cable, alert the poll workers immediately. If a poll worker is

---

<sup>34</sup> Note that the vote data transmitted to the PEB at the closing of a machine is summary vote data instead of raw vote data; that is, it is a summary of the votes recorded rather than each individual electronic ballot as stored inside the iVotronic's internal memory. In order to do a proper recount or error analysis, one would need to remove the CF cards from the iVotronics and seal the CF cards for a precinct with the PEB and any printouts. This information is courtesy of Prof. Doug Jones of the University of Iowa.



## Electronic Voting Machine Information Sheet

disconnecting this cable, it should only be to swap out a printer and you should be able to observe the whole process.

- The PEB device is particularly sensitive. An attacker who gains access to a PEB for a short or extended period of time can change votes on the PEB or attack the central Election Management System when the PEB is returned to election headquarters. PEB devices should only be handled by poll workers and poll workers should keep a vigilant watch over their use of the PEBs throughout the day (that is, they should not be leaving them around casually and the area in which the PEBs are kept should be secure and monitored at all times). If you see a voter or non-poll worker with a PEB, notify election protection immediately.

### Past Problems

**October 2008:** *West Virginia.* Voters in two counties report that incorrect candidates are selected on the iVotronic display screen during early voting.<sup>35</sup>

**October 2008:** *West Virginia.* A ballot programming error by ES&S causes some straight-party votes to register incorrectly for a state Supreme Court race.<sup>36</sup>

**May 2008:** *Arkansas.* Votes for a local Constable race are tallied by iVotronics as part of a state legislative race.<sup>37</sup>

**December 2007:** *Ohio.* A review commissioned by the Ohio Secretary of State found “critical security vulnerabilities” in the iVotronic. The iVotronic can be accessed and manipulated by a person using only a magnet and a personal digital assistant.<sup>38</sup>

**November 2006:** *Florida.* An abnormally high undervote is reported by iVotronics in Sarasota County's Florida's 13th Congressional District race, as well as in other races in six Florida counties that used iVotronics.<sup>39</sup>

**November 2006:** *North Carolina.* Real-Time Audit Log printers fail on almost 10 per cent of machines in Guilford County.<sup>40</sup>

---

<sup>35</sup> “More W. Va. voters say machines are switching votes.” THE CHARLESTON GAZETTE, October 18, 2008. <http://www.sundaygazette.com/News/200810180251>

<sup>36</sup> “Programming glitch affects ballots statewide.” THE CHARLESTON GAZETTE, October 14, 2008. <http://wvgazette.com/News/200810140330>

<sup>37</sup> <http://blog.wired.com/27bstroke6/2008/05/arkansas-voting.html>

<sup>38</sup> EVEREST Academic Review Team Findings, page 51 (page 69 of pdf),

<http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf>

<sup>39</sup> [http://www.votetrustusa.org/index.php?option=com\\_content&task=view&id=2383&Itemid=113](http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2383&Itemid=113)

<sup>40</sup> “Printers failed on voting machines.” NEWS-RECORD, December 15, 2006, *archived at* <http://www.votersunite.org/article.asp?id=6948>



## Electronic Voting Machine Information Sheet

**October-November 2006:** Reports of vote-flipping<sup>41</sup> in Texas, Indiana, Pennsylvania, Florida, and South Carolina: “*Douglas Jones, a computer scientist at the University of Iowa, says he's heard similar stories from voters in several states, including one computer scientist in South Carolina who said that his attempts to vote for one candidate on the iVotronic were repeatedly changed to an opposing candidate by the time he got to the voter verification screen.*”<sup>42</sup>

**November 2004:** *South Carolina.* Officials can't figure out how to retrieve 200 electronic votes from a malfunctioning iVotronic electronic voting machine.<sup>43</sup>

**October 2004:** *North Carolina & Texas.* Voters' choices register incorrectly on the touch screen.<sup>44</sup>

**August 2004:** *Florida.* The iVotronic touch-screen machines -- the ones with the software bugs that caused an uproar the previous May -- showed evidence of the same problems in the August primary. Not only was the low battery problem (which ES&S claimed was repaired) still impacting the elections, problems also showed up with the features that are supposed to allow blind voters to vote independently. The county received 14,253 voter complaint forms about these and other election-day problems.<sup>45</sup>

**January 2004:** *Florida.* In a special election for the State House District 91 seat, with only one item on the ballot, ES&S electronic voting machines showed a total of 134 undervotes – that is, 134 ballots in which voters did not select a candidate even though it was a single-race election. The winner received 12 more votes than the runner-up. Florida law requires a manual recount of invalid votes when the winning margin is less than one quarter of one percent. However, election officials determined that no recount was required because the 134 invalid votes were cast on electronic voting machines, and there is no record of the original votes.<sup>46</sup>

**May 2003:** *Florida.* An internal review of election results by a Miami-Dade county election official found that a DRE system sold by ES&S and used in the May 20, 2003 North Miami Beach runoff election (as well as in earlier elections) was “unusable” for auditing, recounting or certifying an election due to a “serious bug” in the software.<sup>47</sup>

---

<sup>41</sup> “E-voting Failures in the 2006 Mid-Term Elections.” Joint Report by VotersUnite, VoteTrustUSA, Pollworkers for Democracy, Voter Action. <http://www.votetrustusa.org/pdfs/E-VotingIn2006Mid-Term.pdf>

<sup>42</sup> “All Four Major E-voting Machines Flip Votes in Early Voting.” By Warren Stewart.

<http://www.votetrustusa.org/pdfs/E-VotingIn2006Mid-Term.pdf>

<sup>43</sup> Id.

<sup>44</sup> Id.

<sup>45</sup> Id.

<sup>46</sup> “Electronic Vote Recount Stumps Broward Officials.” SUN-SENTINEL, January 10, 2004.

<sup>47</sup> “Count Crisis? Election Officials Warn of Glitches that May Scramble Vote Auditing.” MIAMI DAILY BUSINESS REVIEW, May 16, 2004. “Glitch Forces Change in Vote Audits.” THE MIAMI HERALD, May 15, 2004.



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

**November 2002:** *North Carolina.* At two early-voting locations in Wake County, North Carolina (Raleigh), iVotronics failed to record 436 ballots. This was due to a problem in the firmware of the machines.<sup>48</sup> Firmware is a kind of software loaded on read-only memory so that it cannot be easily changed.

**October 2002:** *Texas.* Democrats said they received several dozen complaints from people who said that they selected a Democratic candidate but that their vote appeared beside the name of a Republican on the screen. Some votes cast for Republicans were counted for Democrats.<sup>49</sup>

**September 2002:** *Florida.* A spot check of machines revealed two problems. First, several Miami-Dade precincts, each with hundreds of voters, are listed as showing one or even no votes cast on election day. Second, differences arose within the same precincts between vote totals produced by the main tabulation system and a backup system.<sup>50</sup>

---

<sup>48</sup>“Electronic Ballots Fail To Win Over Wake Voters, Election Officials; Machines Provide Improper Vote Count At Two Locations,” WRAL-TV RALEIGH-DURHAM, Nov. 2, 2002.

<sup>49</sup>“Area Democrats say early votes miscounted,” THE DALLAS MORNING NEWS, Oct. 22, 2002.

<sup>50</sup>“Leahy: Unskilled workers to blame,” MIAMI HERALD, Sept. 12, 2002.

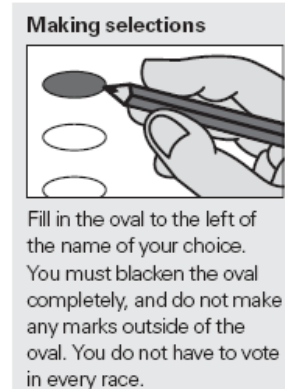


## Electronic Voting Machine Information Sheet ES&S M100 Optical Scan System

**Name/Model:** ES&S Model 100 Optical Scan System

**Maker:** Election Systems & Software

**Voter-Verifiable Paper Trail Capability:** Uses paper ballots



**Brief Description:** The ES&S Model 100 is a precinct-based, voter-activated paper ballot counter and vote tabulator. The ES&S 100 uses visible light scanning to count and record voter information from paper ballots. The ES&S possesses the capability to recognize and alert voters to over and undervoting errors, allowing them to make changes to their ballots. When the polls close, the ES&S Model 100 prints out the voter logs so election officials can have a paper tally.<sup>51</sup>

**Detailed Voting Process:** The ES&S Model 100 functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter then shades in the paper ballot with any standard pen or pencil and inserts the ballot into the ES&S Model 100, where they are given a chance to review their votes. As votes are entered, the ES&S Model 100 stores the vote tallies on its internal memory card. When the polls close, the ES&S Model 100's internal printer prints out the precinct's vote report on paper.<sup>52</sup>

### What to Look For

- **Security Seals.** Ideally, the M100's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like

<sup>51</sup> From the manufacturer's website, available at: <http://www.essvote.com/HTML/products/m100.html>

<sup>52</sup> From the manufacturer's product brochure, available at:  
<http://www.essvote.com/HTML/docs/Model100.pdf>



## Electronic Voting Machine Information Sheet

this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should be locked and/or be sealed with tamper-evident tape.
- **The Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.
- **Keys.** The keys for the M100 are the same for all M100 machines and are easily pickable with readily available tools. Care should be observed around the ballot box lock and the scanner key lock (turns the system off and on).
- **Counterfeit ballots.** It is fairly easy to frustrate the counterfeit ballot detection mechanism on the M100. People who produce counterfeit ballots could cast multiple votes and the detectability of these ballots would only depend on how close they appeared to be like the real ballot cards.

### Past Problems:

The ES&S Model 100 has many reported problems, ranging from unidentifiable malfunctions in a Hawaii election, to missing votes in 98% of precincts in a Texas election, to substantial delays in accepting ballots and returning election results in Rhode Island, to flawed ballot data causing serious election irregularities in another Texas election.

These problems have been encountered across multiple versions of the machine and its operating system and after multiple certification processes.<sup>53</sup>

---

<sup>53</sup> From the VotersUnite webpage, available at: <http://www.votersunite.org/info/ES&Sinthnews.pdf>



## Electronic Voting Machine Information Sheet

### ES&S Optech III-P Eagle (also Sequoia Optech III-P Eagle)

**Name/Model:** Optech III-P Eagle

**Maker:** Sequoia Voting Systems

**Voter-Verified Paper Record Capability:** Uses paper ballots



**Brief Description:** As an optical ballot tabulator, the Optech III-P Eagle functions at the precinct level. The Optech III-Eagle consists of an electronic ballot counting device which reads completed ballots by scanning for the voters' marks indicating their voting preferences. The Optech III-Eagle then tabulates the results. When the polls close, the results are both printed on a paper copy and stored to an internal memory card.<sup>54</sup>

The Optech III-Eagle runs off both internal and external power to reduce the risk of malfunctions, and it can store voter data on an internal memory card, transmit data via phone lines or satellite, and it can print out paper copies of voter results.

**Detailed Voting Procedure:** The Optech III-Eagle functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter shades in the paper ballot with any standard pen or pencil and inserts the ballot into the Optech III-Eagle, which then ensures that the ballot has been properly marked and that no over or under voting has occurred. As votes are entered, the Optech III-Eagle stores the vote tallies on its internal memory card., and when the polls close, the Optech III-Eagle prints out a paper copy of the election results for polling officials.<sup>55</sup>

<sup>54</sup> From the manufacturer's website, available at: <http://www.sequoiavote.com/bEAGLE.php>

<sup>55</sup> From the manufacturer's website, available at: <http://www.sequoiavote.com/bEAGLE.php>



## Electronic Voting Machine Information Sheet

### What to Look For

- **Security Seals.** Ideally, the Eagle's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should be locked and/or be sealed with tamper-evident tape.
- **Keys.** The keys for the Optech III-P Eagle are the same for all Optech III-P Eagle machines and are easily pickable with readily available tools. Care should be observed around the ballot box lock and the scanner key lock (turns the system off and on).
- **The Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some models of the Eagle have trouble reading red inks or inks with red in them. These Eagles use an infrared lamp to detect voting marks and red or reddish inks appear "blank" under this light. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.

### Past Problems:

There have been some reported problems with the Optech III-Eagle, although not as many as with other systems, although this may be because of the relative newness of the system. One known issue is that there can be compatibility problems between the Optech III-Eagle and other Sequoia Voting Systems, such problems having led to tabulation delays and errors in a multiple cities in the Wisconsin primary elections in 2006.<sup>56</sup>

---

<sup>56</sup> Compiled from various news reports, from the VoteTrustUSA website, available at: [http://www.votetrustusa.org/index.php?option=com\\_content&task=view&id=1793&Itemid=113](http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1793&Itemid=113)



## Electronic Voting Machine Information Sheet

### Hart Intercivic eScan

**Name/Model:** e-Scan

**Manufacturer:** Hart InterCivic

**Voter-Verified Paper Record Capability:** Uses paper ballots



**Brief Description:** The eScan is a precinct-based, digital ballot scanning system. After marking a paper ballot, the voter feeds it directly into the eScan at the precinct. The ballot image is stored as a *Cast Vote Record* on a flash memory card that can be retrieved and tabulated when the polls close. eScans can be programmed to reject over-voted, under-voted and blank ballots, thereby providing second-chance voting at the precinct.<sup>57</sup>

**Detailed Voting Process:** The Hart InterCivic E-Scan system functions much like a traditional paper balloting system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter then shades in the boxes on the paper ballot (above right) with any standard pen or pencil and inserts the ballot into the e-Scan machine.

**Past Problems:** Not many problems have been reported on the operation of the Hart InterCivic E-Scan. However, the E-Scan has been known to have problems reading creased ballots.<sup>58</sup> Most of the reported problems are with the e-Slate system, which uses an entirely different technology.

<sup>57</sup> From the manufacturer's website, available at: <http://www.hartintercivic.com/files/hartfacts>

<sup>58</sup> Citing a Colorado newspaper article.

[http://www.votetrustusa.org/index.php?option=com\\_content&task=view&id=322&Itemid=51](http://www.votetrustusa.org/index.php?option=com_content&task=view&id=322&Itemid=51)



## Electronic Voting Machine Information Sheet

Hart InterCivic recently made news by agreeing to comply with a trusted voting open-source mandate, meaning that they will allow their software to be examined for flaws by interested parties.<sup>59</sup>

### Things to Look Out For

- **Security Seals.** Ideally, the eScan's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Ballot Box Access.** Optical scan systems have at least one and possibly more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should be locked and/or be sealed with tamper-evident tape.
- **The Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.
- **Ethernet port.** Although mentioned above, we need to emphasize that the ports on the eScan should be protected from tampering at all times, and preferably disabled. An attacker could use these ports to replace the software on the eScan, swap votes, and/or change results.

---

<sup>59</sup> For more details, go to:

[http://www.votetrustusa.org/index.php?option=com\\_content&task=blogcategory&id=75&Itemid=179](http://www.votetrustusa.org/index.php?option=com_content&task=blogcategory&id=75&Itemid=179)



## Electronic Voting Machine Information Sheet

### Hart InterCivic eSlate

**Name / Model:** eSlate 3000<sup>60</sup>

**Vendor:** Hart InterCivic, Inc.

**Voter-Verifiable Paper Record Capability:** Yes<sup>61</sup>



**Brief Description:** Hart InterCivic's eSlate is a multilingual voter-activated electronic voting system where the voter turns a Select Wheel and pushes a button to indicate his/her preference. The eSlate is connected via serial cable to the Judge's Booth Controller (JBC; image above) which provides vote activation and vote storage for up to twelve eSlates. A poll worker issues a four digit, randomly generated Access Code to the voter using the JBC. The voter enters the Access Code on the eSlate and votes using the select Wheel and Buttons. Once the ballot is cast, the votes are stored in redundant and physically separate areas of the eSlate System, including the eSlate, JBC and flash memory. The votes are transmitted via a cable to the JBC, and are stored on the JBC and on a flash memory card (Mobile Ballot Box or MBB) inside the JBC. Then the MBB is physically transported to election headquarters for tabulation.

**Checking the Voter-Verifiable Paper Trail:** The voter-verifiable paper trail for the eSlate is called the Verified Ballot Option (VBO). The VBO printer is a reel-to-reel, cash-register style of printer. The VBO printout is found to the left of the display screen under transparent plastic. The VBO is a sealed unit that must be changed entirely when the unit runs out of paper, jams, etc.

<sup>60</sup> See: <http://www.hartintercivic.com/innerpage.php?pageid=26>

<sup>61</sup> Where available. eSlates in California include a vvpap printer. In Indiana, Kentucky, Pennsylvania, Tennessee, Texas and Virginia, no printer is used.



## Electronic Voting Machine Information Sheet

**Detailed Voting Process:** When the voter enters the precinct, poll workers first confirm that the voter is properly registered. Then, a poll worker using the Judge's Booth Controller (JBC) prints out a piece of paper with a four digit, randomly generated Access Code. This number does not tie to the voter's identity but ties to the voter's precinct so that the proper ballot style for each voter will appear on the eSlate after a voter enters his/her Access Code. A voter is NOT assigned to any specific voting terminal. A voter can proceed to any open eSlate booth.

The voter takes the piece of paper with the Access Code to any open eSlate booth and enters the number into the eSlate device using the Select Wheel and Enter button. This Access Code number permits the voter to vote once; the Access Code will not work a second time. The voter makes his or her selections using the buttons and Select Wheel on the bottom of the eSlate. The Select Wheel allows the voter to navigate through the ballot. When the voter is finished, he or she presses the red "Cast Ballot" button at the lower left-hand corner of the eSlate to cast his/her ballot. Access Codes cannot be reissued by the JBC.

It is possible for a voter to ask a poll-worker if his/her Access Code has registered a ballot on the JBC. If the voter has completed the voting process and cast a ballot, the poll worker can print off a piece of paper similar to the Access Code that lists the voter's Access Code number and reads "Assigned and Cast." Again the Access Code is a randomly generated number and does not tie to the identity of the voter.

The ballot is then transmitted over the cable that connects the eSlate to the JBC on a closed, private network. This cable is a "serial" cable and carries both power and data. Up to twelve eSlates can be connected via this serial cable to the JBC. The JBC records and stores the ballot internally and on a flash memory card or Mobile Ballot Box (MBB). Additionally, each ballot is stored on the individual eSlate voting unit so that all ballots are stored redundantly in separate areas of the eSlate System. The MBB is a removable PCMCIA computer card that stores vote data as well as the ballot definitions and election-specific information needed to open the polls for an election. The PCMCIA card is a credit card-sized device containing flash memory that is sealed into a slot on the JBC.

Once the balloting is closed, the poll workers use the printer on the JBC to print summary results on to paper. Then the poll workers either remove the MBB and physically transport it with any printouts to a central tabulation facility or they can transport the JBC itself depending on local regulations and procedures.

### Things to Look Out For

- Security Seals. Ideally, the eSlate's and JBC's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached



## Electronic Voting Machine Information Sheet

under controlled, explained circumstances. A voided seal looks like this:  
<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- Cables must be secured. The eSlate system is daisy-chained system where the JBC controls multiple eSlate terminals. The places where the first cable connects to the JBC as well as the area on the top of each eSlate where two of these cables connect are particularly sensitive. The last eSlate on the “daisy-chain” – likely the eSlate farthest from the JBC – is especially sensitive as it will have one cable coming from another eSlate, but will also have an exposed serial cable port. A malicious party could connect their own cable or device to this exposed port and essentially take control of the election, the software in the eSlate and JBC as well as vote data stored locally on each eSlate and remotely on the JBC. Ideally, this last exposed serial port will be covered or otherwise disabled. Jurisdiction should use security seals or protected serial cables that cannot be easily disconnected by voters (granted, this might make them difficult for poll workers to connect and disconnect).
- VBO is Sensitive and Sealed. The VBO, Hart’s VVPAT subsystem, is a sealed unit that stores official vote data. The unit should not be opened or serviced except infrequently under monitored and controlled circumstances so that all security seals are logged and reapplied. The entire VBO unit should be replaced when an error or jam occurs. The VBO, if jostled out of its place, can be made to interrupt or duplicate printing.
- JBC and JBC Ports are Sensitive. The JBC controller and the ports on the back of the JBC are sensitive. With access to the JBC, access codes can be printed out to allow duplicate voting. The ports on the back of the JBC should be covered or otherwise disabled. With access to these ports, a malicious party could take control of the election, activate arbitrary numbers of voter Access Codes, cast votes, erase votes and other things. Access to the JBC and to the area in the back of the JBC control panel where these ports reside should be monitored and controlled at all times.
- The MBB Memory Card is Sensitive. Corrupt MBB cards can introduce viruses, cause the main election server to crash and falsify votes. Access to the MBB memory card should be controlled, monitored and logged at all times.

## Past Problems

**October 2008:** *Tennessee*. The Ballot Summary Page displays only the first three letters of the candidates' names, confusing some voters.<sup>62</sup>

---

<sup>62</sup> “Voting machine issue confusing to some voters.” Knoxnews.com, October 22, 2008, <http://www.knoxnews.com/news/2008/oct/22/voting-machine-issue-confusing-some/>



## Electronic Voting Machine Information Sheet

**December 2007:** An expert review commissioned by the Secretary of State of Ohio finds there are “insufficient protections within the Hart voting equipment and software to prevent a motivated adversary from compromising an entire election.”<sup>63</sup>

**August 2007:** An expert review commissioned by the Secretary of State of California finds serious security issues in the eSlate and the supporting county server system. The Secretary allows the eSlate to remain a primary voting system with new chain of custody and manual auditing requirements.<sup>64</sup>

**October 2006:** *California.* Trained personnel entering test votes on the eSlate made errors on 40% of the test ballots in the first day of testing; 25% of the ballots the second day; and 14% the third day.<sup>65</sup>

**March 2006:** *Texas.* Computer programming errors added 100,000 votes to the final tallies in both primaries, leading to multiple candidate requests for recounts.<sup>66</sup>

**October 2004:** *Texas.* A “default” selection is a selection automatically pre-set by the software. It remains selected unless the user specifically chooses to change it. To provide a default selection on a DRE voting machine is to give a voter a ballot with a candidate already marked. Yet, election officials in Austin set up the eSlate DREs with Bush/Cheney as the default choice for president/vice-president. Voters who voted a straight party Democratic ticket watched their presidential votes changed to Bush on the review screen. Officials said voters caused this by pressing the “Enter” button on the second screen of the eSlate machine.<sup>67</sup>

**September 2004:** *Hawaii.* Precincts offered both optical scan ballots and new eSlate paperless machines. eSlate malfunctions disenfranchised at least one voter. Most people chose not to use the eSlates. New eSlate electronic voting machines allowed voters to choose a Green Party ballot, even though there were no Green Party candidates. 22 voters were disenfranchised by the error.<sup>68</sup>

**March 2004:** *California.* Hundreds of voters in Orange County were turned away when one eSlate machine broke down. It is not clear from reports if this was a JBC or eSlate.<sup>69</sup>

**March 2004:** *California.* Approximately 7,000 voters were presented with the wrong ballots due to problems with poll workers’ understanding the eSlate system. In 21

---

<sup>63</sup> EVEREST Voting System Review, Academic Team findings, Secretary of State of Ohio, p. 213 (p.231 of pdf). <http://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf>

<sup>64</sup> Hart InterCivic Voting System, Withdrawal of Approval/Conditional Reapproval, Secretary of State of California, December 6, 2007 Revision, [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/hart\\_amended\\_recert\\_final\\_120707.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/hart_amended_recert_final_120707.pdf)

<sup>65</sup> See <http://www.votersunite.org/info/HArtinthenews.pdf>

<sup>66</sup> Id.

<sup>67</sup> Id.

<sup>68</sup> Id.

<sup>69</sup> “Voters Decide Record Bond Issue; Edwards Quits.” NBC4TV, March 2, 2004.



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

precincts where the problem was most acute, more ballots were cast than there were registered voters. Tallies at an additional 55 polling places with turnouts more than double the county average of 37% suggest at least 5,500 voters had their ballots tabulated for the wrong precincts.<sup>70</sup>

**February 2004. Virginia.** Voters had to cast paper ballots when the JBC unit at one precinct “fried,” rendering all the eSlate machines unusable.<sup>71</sup>

**November 2003: Texas.** Poll workers in Harris County, confused by the eSlate system's complexity, could not get the machines to work properly. Subsequent investigation revealed they had been assigning the wrong ballots to voters using the JBC.<sup>72</sup>

---

<sup>70</sup> “7,000 Orange County Voters Were Given Bad Ballots.” LOS ANGELES TIMES, March 8, 2004.

<sup>71</sup> “Polling places report light turnout here,” RICHMOND TIMES-DISPATCH, February 11, 2004.

<sup>72</sup> “ESlate voting proves smooth, not flawless.” HOUSTON CHRONICLE, Nov. 5, 2003.



## Electronic Voting Machine Information Sheet

### Microvote, Inc. MV/464

**Name / Model:** MV / 464

**Vendor:** MicroVote

**Voter-Verifiable Paper Record Capability:** None



**Brief Description:** This model is no longer in production. It is a push-button style direct recording electronic (DRE) device, which records the votes cast into a data cartridge. At the end of the election, the data cartridge is removed and transported to the central tabulation facility, where it is inserted into a cartridge reader attached to a PC running vendor-supplied software. It is used in Indiana, Kentucky, and one Tennessee county.

**Detailed Voting Process:** The voter makes each candidate selection by pressing the gray button beside a candidate's name. This turns a light on next to the button. To change a selection, a voter presses the gray button a second time, and the light turns off.

The voter may navigate forward through ballot screens by pressing the green "Advance Ballot" bar at the bottom of the panel. The voter may navigate back through ballot screens by pressing the blue "Review Ballot" bar at the bottom of the panel. The voter must view all pages of the ballot before the machine will allow a vote to be cast.

To cast a write-in vote, the voter presses the gray write-in selection button on the bottom left side of the panel. The light next to it will start blinking. The voter then writes in the desired name on the paper tape in the write-in window, also at the bottom left of the panel. The voter may change his or her mind by pressing the same write-in button again to turn out the light, and then vote as usual.

To cast the ballot, the voter presses the red "Cast Vote" button on the bottom right side of the panel.



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

### Things to Look Out For

- Security Seals. Ideally, the MV-464's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this:  
<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

### Past Problems

**November 2003: Indiana** – Electronic vote-tabulation equipment reported that 140,000 votes had been cast in a county of 50,000 residents, due to a problem with DOS based software on the computer that used the CI-4800 Cartridge Reader to read the votes.<sup>73</sup>

---

<sup>73</sup> "Voting Machine Glitch Shows Thousands of Extra Votes," Grant Gross, IDG News Service, 11/03/2003, <http://www.itworld.com/031113votingglitch>.



## Electronic Voting Machine Information Sheet

### Microvote, Inc. Infinity

**Name / Model:** Microvote Infinity  
**Vendor:** MicroVote General Corporation  
**Voter-Verified Paper Record Capability:** None



**Brief Description:** The Microvote Infinity is a direct-recording electronic (DRE) voting machine. Unlike many DREs now in use, the Infinity is a push-button, rather than a touch screen, voting machine. This system is used in Indiana and Tennessee.

**Voting on the Microvote Infinity:** The voter makes each candidate selection by pressing the gray button beside a candidate's name. An "X" will then appear next to the candidate's name. If the voter wishes to change her selection, she presses the button next to the candidate's name a second time, which de-selects the candidate. The voter navigates through the ballot by pressing a "Next Page" button on the lower right of the display panel, and can review her ballot by pressing a "Previous Page" button on the lower left of the panel. To cast a write-in vote, the voter presses the gray write-in selection button, and then presses the buttons next to the letters in the candidate's name. When the voter is ready to cast her vote, she presses a red "Cast Vote" button on the right side of the display panel.<sup>74</sup>

If a voter is using a wheelchair or does not believe she will be able to stand at the machine long enough to complete the voting process, the Infinity display panel can

---

<sup>74</sup> How to Cast Your Vote with Microvote Infinity. Office of the Tennessee Secretary of State.  
[http://tn.gov/sos/election/voting\\_systems/microvote.pdf](http://tn.gov/sos/election/voting_systems/microvote.pdf)



## Electronic Voting Machine Information Sheet

detach, and the voter can hold the panel in her lap. For voters with vision disabilities, the Infinity has an audio functionality called DoubleTalk. The DoubleTalk module is connected to the Infinity's communications port before the poll worker inserts the voter card. A voter may bring her own headphones to use, or use the headphones supplied with the DoubleTalk module. The DoubleTalk module will instruct the voter on how to navigate through her ballot using the same buttons used by all voters.<sup>75</sup>

### Things to Look Out For

- Security Seals. Ideally, the Infinity's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- The Infinity has exterior communication ports (RJ45, like Ethernet connectors) that may or may not be sensitive. Unfortunately, there has been no publicly disclosed independent evaluation of the Infinity, so it is difficult to say if an attacker could connect to the terminal via these ports. Ideally, these ports would be covered or disabled during voting.
- The Infinity uses an 8MB CompactFlash card to store vote data. If this card is easily accessible, it could be a sensitive area of the Infinity. Unfortunately, we are uncertain as to how the CompactFlash card is inserted and removed from the Infinity.

### References

Useful system information on the Infinity is available here: MicroVote General Corporation Election Management System (EMS) Voting System v. 4.0.0 VSTL Certification Test Plan. (2007). iBeta Quality Assurance. Retrieved October 24, 2008, from [http://www.eac.gov/voting%20systems/docs/certification-docs-vstl-test-plan\\_emsv-4-0-0-v-2-0.pdf/attachment\\_download/file](http://www.eac.gov/voting%20systems/docs/certification-docs-vstl-test-plan_emsv-4-0-0-v-2-0.pdf/attachment_download/file).

---

<sup>75</sup> Voting System Training Video: Infinity by Microvote. Office of the Indiana Secretary of State. Available at: <http://www.in.gov/sos/elections/hava/pollworkertraining.html>



## Electronic Voting Machine Information Sheet

### Premier Election Solutions AccuVote-OS

**Name/Model:** AccuVote-OS Optical Scan System

**Maker:** Premier Election Solutions (formerly Diebold)

**Voter-Verified Paper Record Capability:** Uses paper ballots



**Description:** AccuVote-OS is a precinct and central accumulation optical scan voting system. The AccuVote is a small system, and can be transported without excessive difficulty.

When using the AccuVote-OS as a precinct based optical scan unit, ballots are processed in the polling place, not transported to a central location. Only the voter touches the ballot between the time it is cast and the time it is counted. The AccuVote-OS integrates the vote tabulation and recording process into one unit. The unit is powered with both an internal battery source and an external source. The AccuVote-OS is currently in use in 900 jurisdictions.<sup>76</sup>

**Detailed Voting Process:** The AccuVote-OS functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter shades in the paper ballot with any standard pen or pencil and inserts the ballot into the AccuVote-OS, where they are given a chance to review their votes.<sup>77</sup> As votes are entered, the AccuVote-OS stores the vote tallies on its internal memory card.<sup>78</sup> When the polls close, the AccuVote-OS then transmits the voting data from the polling place to the central host computer by way of a modem.<sup>79</sup>

### What to Look For

- Security Seals. Ideally, the OS's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached

<sup>76</sup> <http://verifiedvoting.org/verifier>

<sup>77</sup> Source Code Review of the Diebold Voting System, Office of the Secretary of State of California Top-to-Bottom Review, [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/diebold-source-public-jul29.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf)  
[http://www.diebold.com/dieboldes/pdf/dieboldes\\_OS\\_brochure.pdf](http://www.diebold.com/dieboldes/pdf/dieboldes_OS_brochure.pdf)

<sup>78</sup> Id.

<sup>79</sup> Id.



## Electronic Voting Machine Information Sheet

under controlled, explained circumstances. A voided seal looks like this:  
<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- **Keys.** The keys for the AccuVote-OS are the same for all AccuVote-OS machines and are easily pickable with readily available tools. Care should be observed around the ballot box lock and the scanner key lock (turns the system off and on).
- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should be locked and/or be sealed with tamper-evident tape.
- **The Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.

### Past Problems:

Multiple problems have been encountered in a variety of jurisdictions, ranging from incorrect total vote counts in Barry County, Michigan, to not accepting ballots in King County, Washington, to delays in Putnam County, Georgia due to inaccuracies in the memory card totals.<sup>80</sup> The problems have been encountered across multiple versions and after multiple certification procedures. See also the October, 2006 University of Connecticut VoTeR Center and Department of Computer Science and Engineering report here: <http://voter.engr.uconn.edu/voter/Report-OS.html>

---

<sup>80</sup> From the VotersUnite! website: <http://www.votersunite.org/info/Dieboldinthenews.pdf>



## Electronic Voting Machine Information Sheet

### Premier Election Solutions AccuVote-OSX

**Name/Model:** Accuvote-OSX Digital Scan System

**Maker:** Premier Election Solutions (formerly Diebold Election Systems)

**Voter-Verifiable Paper Trail Capability:** Uses voter-marked paper ballots



[photo from Premier: [http://www.premierelections.com/documents/product\\_sheets/Accuvote-OSX.pdf](http://www.premierelections.com/documents/product_sheets/Accuvote-OSX.pdf)]

**Description:** Accuvote-OSX is a precinct and central accumulation optical scan voting system. When using the Accuvote-OSX as a precinct based digital scan unit, ballots are processed in the polling place, not transported to a central location. Only the voter touches the ballot between the time it is cast and the time it is counted. The Accuvote-OSX integrates the vote tabulation and recording process into one unit. The unit is powered with both an internal battery source and an external source.

**Detailed Voting Process:** The Accuvote-OSX functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter shades in the paper ballot with any standard pen or pencil and inserts the ballot into the Accuvote-OSX, where they are given a chance to review their votes. As votes are entered, the Accuvote-OSX stores the vote tallies on its internal memory card.<sup>81</sup> When the polls close, the Accuvote-OSX then transmits the voting data from the polling place to the central host computer by way of a modem.<sup>82</sup>

### What to Look For

- Security Seals. Ideally, the OSX's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only

<sup>81</sup> [http://www.premierelections.com/documents/product\\_sheets/Accuvote-OSX.pdf](http://www.premierelections.com/documents/product_sheets/Accuvote-OSX.pdf)

<sup>82</sup> [http://www.premierelections.com/documents/product\\_sheets/Accuvote-OSX.pdf](http://www.premierelections.com/documents/product_sheets/Accuvote-OSX.pdf)



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should locked and/or be sealed with tamper-evident tape.
- **The Memory Card is Sensitive.** Corrupt memory cards may be able introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, black ballpoint pen that does not bleed through paper.

### Past Problems:

**October 2008:** *Florida.* The tolerances of the OSX are such that the machine rejects ballots produced by Ballot on Demand printers.<sup>83</sup>

---

<sup>83</sup>“Lines, Voting Problems Continue on 2<sup>nd</sup> Day.” Channel 4 News, Jacksonville, FL.  
<http://www.news4jax.com/news/17770664/detail.html>



## Electronic Voting Machine Information Sheet

### Premier Election Solutions AccuVote-TSx

**Name / Model:** AccuVote / TSx<sup>84</sup>

**Vendor:** Premier Election Solutions (formerly Diebold Election Systems)

**Voter-Verified Paper Record Capability:** Yes.<sup>85</sup>



**Brief Description:** The AccuVote-TSx is a touch screen direct-recording electronic (DRE) voting machine. It is a multilingual voting system activated by a smart card and records votes on internal flash memory. Voters insert a "smart-card" into the machine and then make their choices by touching an area on a computer screen, much in the same way that modern ATMs work. AccuVote-TSx offers a summary page once the voter has sequenced through the entire ballot, giving the voter an opportunity to verify their choices and to vote in any race they missed. The votes are then recorded to internal electronic memory. If the optional AccuVote Printer Module (AccuView) is attached, voters have the opportunity to view a printed ballot under a transparent screen, and compare this paper record with the adjacent electronic summary screen. When polls close, the votes for a particular machine are written to a "PCMCIA card," which is removed from the system and either physically transported to election headquarters or their contents transmitted via computer network. Voter-verifiable paper records are removed from their enclosure in the AccuView housing and likewise transported to election headquarters.

**Checking the Voter-Verifiable Paper Trail:** If the TSx is equipped with the voter-verifiable paper trail, the printer tape is located to the right of the touch screen, viewable under transparent plastic. Many, but not all, TSx machines in use are equipped with printer module. In Texas, Pennsylvania, Virginia, and Tennessee, the TSx systems are not equipped with the paper-trail printer.

**Detailed Process:** When the voter enters the precinct, he or she is given a "smartcard" by a poll worker after confirming the voter is registered. A "smart-card" is a card the size and shape of a credit-card which contains a computer chip, some memory and basic data

<sup>84</sup> See [http://www.diebold.com/dieboldes/solutions\\_management\\_tsx.asp](http://www.diebold.com/dieboldes/solutions_management_tsx.asp)

<sup>85</sup> With the optional [AccuView Printer Module™](#)



## Electronic Voting Machine Information Sheet

such as the voter's voting language and political party. The voter then takes the smart-card to a voting machine and inserts the smart-card into the machine to allow voting. After using the touch screen to vote, 1) the record of the vote is directly recorded electronically to multiple, internal flash memory cards and 2) the voter's smart-card is reset to ensure that it can only be used to vote once. The smart-card pops out of the machine with a loud "click" and the voter returns it to a poll worker.

If the optional printer module is in use, voting takes place as described above however, at the conclusion of voting, a paper ballot is printed and displayed under a transparent screen in the AccuView housing so that the voter can verify their selections before the ballot is deposited into a container within the printer module to await retrieval by poll workers.

When the polls close, a poll worker or election official inserts a different-type of smartcard, an *administrator* card, into each voting machine and puts the machine into a postelection mode where it will no longer record votes. At this point, the machine writes the votes from its internal memory to flash memory on a "PCMCIA card". The PCMCIA card is merely a removable form of flash memory. A printed tape of all votes cast or vote totals for the voting machine can also be printed out at this time depending on local procedure and regulations.

The PCMCIA cards are taken out of each machine and either taken to a central tabulation facility or to remote tabulation facilities. At the tabulation facility the votes are read out of the PCMCIA cards and into a central computer database where precincts are combined to result in an aggregate vote. For remote facilities, the votes are transmitted to the central tabulation facility via a closed "Intranet", the Internet or modem. The PCMCIA cards and any printouts from the voting machines can then become part of the official record of the election.

### What to Look Out For

- VVPAT cover. There is an opaque cover on hinges over the VVPAT viewing window. This cover is intended to give voters with visual impairment a higher degree of ballot privacy since they use the audio ballot and do not use the VVPAT for verification. Unfortunately, this cover can be shut inadvertently or not re-opened after a voter with sight impairment votes. This cover should always be open unless a disabled voter is using the TSx. In fact, the cover can easily be removed from its hinges and re-attached when necessary.
- Memory cards. The TSx is susceptible to viruses transmitted through its memory card pack. Great care should be taken when handling the memory packs. A voter should never touch, remove or otherwise mess with the TSx memory pack. Poll



## Electronic Voting Machine Information Sheet

workers should only do so after polls have closed and the election closed on each TSx terminal.

- Security seals. Many jurisdictions wisely employ tamper-evident seals to indicate when a machine might have been compromised. These seals look like stickers with serial numbers on them. When removed, they change color or otherwise indicate that the seal is no longer covering the security-sensitive area it was before. To see an example of a seal after it has been removed (thus, voided), see this image: <http://www.flickr.com/photos/joebeone/2247733620/>. It is important than any seal that reads “VOID” or similar that is still in place on a machine be reported immediately to poll workers (and then called into the Our Vote hotline listed at the top of the page). Places to expect security seals include over the power switch or “close polls” button, over the memory card or memory card cover and over the case seams (if someone gains access to the internals of a TSx by removing its case they can install their own software on it).

### Past Problems

**August 2008: Ohio.** State and local election officials find that when memory cards from TSx machines and from Premier optical scan machines are uploaded to the county server, some votes may not be uploaded.<sup>86</sup> The problem lies in the source code of the GEMS election management server (the “county server”) affects almost all of the jurisdictions which use Premier's county server. Premier has advised all of its customers to audit precinct totals and take other steps to avoid uncounted votes.<sup>87</sup>

**August 2007: California.** Following an expert top-to-bottom review of voting systems which finds critical security vulnerabilities in the TSx, and the Secretary of State disallows the machine's use as a primary voting system.<sup>88</sup>

**May 2006: Ohio.** Voter access card failures, paper jams, and even a missing electrical adapter on the touch screen machines caused election problems. Screen review doesn't match ballot printout. Electronic ballot boxes were lost in two counties.<sup>89</sup>

**July 2005: California.** California. After testing 96 touch screen machines and finding a 10% error rate, Secretary of State Bruce McPherson rejected Diebold's application to certify the AccuVote TSx touch screen with AccuView printer module.<sup>90</sup>

---

<sup>86</sup> “E-voting Vendor: Programming Error Cause Dropped Votes,” PC World, August 22, 2008, available at: [http://www.pcworld.com/businesscenter/article/150188/evoting\\_vendor\\_programming\\_errors\\_caused\\_dropped\\_votes.html](http://www.pcworld.com/businesscenter/article/150188/evoting_vendor_programming_errors_caused_dropped_votes.html)

<sup>87</sup> Advisory from Premier Election Solutions to all customers. August 19, 2008, available at: [http://www.votersunite.org/info/premier\\_pan\\_081908.PDF](http://www.votersunite.org/info/premier_pan_081908.PDF)

<sup>88</sup> Secretary of State of California, Premier Election Solutions, Withdrawal of Approval/Conditional Reapproval, October 25, 2007. [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/diebold\\_102507.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold_102507.pdf)

<sup>89</sup> See: <http://www.votersunite.org/info/dieboldinthenews.pdf>

<sup>90</sup> Id.



## Electronic Voting Machine Information Sheet

**April 2004:** *California.* Secretary of State Kevin Shelley decertified all electronic touch-screen voting machines in the state due to security concerns, primarily caused by Diebold.<sup>91</sup>

### References:

Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, & William P. Zeller. (2007). Source Code Review of the Diebold Voting System. California Secretary of State. Retrieved October 23, 2008, from [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/diebold-source-public-jul29.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf) .

“Security Analysis of the Diebold AccuVote-TS Voting Machine ,” Center for Information Technology Policy, Princeton University, September, 2006. See <http://itpolicy.princeton.edu/voting/>. Diebold’s response may be found at <http://www.diebold.com/dieboldes/pdf/princetonstatement.pdf>.

Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, “Analysis of an Electronic Voting Machine”, *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. See: <http://avirubin.com/vote.pdf>

“DRE Security Assessment, Volume 1, Computerized Voting Systems, Summary of Findings and Recommendations,” InfoSENTRY, 21 Nov. 2003. See: <http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf>

“Direct Recording Electronic (DRE) Technical Security Assessment Report,” Compuware Corporation, 21 Nov. 2003. See: <http://www.sos.state.oh.us/sos/hava/files/compuware.pdf>

“Risk Assessment Report: Diebold Accuvote-TS Voting System and Processes (redacted)”, Science Applications International Corporation SAIC-6099-2003-261, Sept. 2, 2003. See: <http://www.dbm.maryland.gov/SBE>

“Trusted Agent Report -- Diebold AccuVote-TS Voting System,” RABA Technologies, Jan. 20, 2004. See: [http://www.raba.com/text/press/TA\\_Report\\_AccuVote.pdf](http://www.raba.com/text/press/TA_Report_AccuVote.pdf)

---

<sup>91</sup> Id.



**Electronic Voting Machine Information Sheet**  
**Sequoia Voting Systems AVC Advantage**

**Name / Model:** AVC / Advantage<sup>92</sup>

**Vendor:** Sequoia Voting Systems, Inc.

**Voter-Verifiable Paper Record Capability:** None.<sup>93</sup>



**Brief Description:** The AVC Advantage is a poll worker-activated full-face direct recording electronic voting system with a touch-sensitive matrix of switches that voters push to indicate their choices. Voting records are recorded internally to battery-powered RAM. Poll workers activate the machine using an operator panel on the side of the machine to choose the ballot style and voters make choices by touching a black arrow next to their choice. A record of the vote is then recorded internally to three sets of battery-powered RAM memory. When polls are closed, poll workers remove a cartridge of battery-powered RAM that contains the vote records from each machine. These cartridges are then either physically transported to a tabulation facility or their contents transmitted over modem.

**Detailed Voting Process:** The voter enters the polling place and is given a voting ticket after confirming that the voter is registered. The voting ticket is a colored piece of paper with two identical and unique numbers.<sup>94</sup> The voter hands their ticket to a poll worker operating an Advantage voting machine and then tears the voting ticket in half and hands one half back to the voter. The poll worker uses an operator's panel on the side of the

<sup>92</sup> <http://www.sequoiavote.com/productguide.php?product=AVC%20Advantage&type=Introduction>

<sup>93</sup> In 2005 NJ passed a law requiring voter-verifiable paper records which will take effect in 2009. Printers developed for NJ were tested in 2007 but failed initial tests. (Advocates have urged a switch to precinct-count optical scan.) CO's law takes effect 2010. LA, PA and VA have no such requirement.

<sup>94</sup> The two numbers on the ticket are not tied in any way to the voter other than ballot style.



## Electronic Voting Machine Information Sheet

machine to choose the ballot style appropriate for that voter depending on the color of their voting ticket.<sup>95</sup> The voter enters the curtains (see picture above) and verifies that their ballot is the right one by comparing the color of their ticket to a LCD screen in the lower-right corner of the front of the voting machine. Then the voter votes by pressing a black arrow next to each choice in each race on the ballot. Blinking lights above each race indicate that no choice has been made in that race. If the voter tries to choose more than one choice in a given race (over-voting), the machine will ignore the second choice. To change a selection, voter can press the black arrow by the incorrect choice to deselect it, then select the correct choice.

When done voting, the voter presses a “Cast Vote” button in the lower-right corner of the voting machine. It is very important that the voter does not push the vote-casting button until they are done voting; a vote inadvertently cast can likely not be redone.<sup>96</sup> The vote is recorded internally to three sets of battery-powered RAM, one of which is on a removable cartridge.<sup>97</sup> The vote records are stored in a manner similar to a ballot image.<sup>98</sup>

When the polls close, poll workers remove cartridges of battery-powered RAM containing the vote records from each machine. At this point, depending on local election procedure and regulations, the cartridges can either be physically transported to a tabulation facility or their data can be sent over a modem. At the tabulation facility, the votes from all cartridges and precincts are read into vote tabulation databases and combined to result in an aggregate vote tally. In order to send vote records over a modem, a cartridge reader must read out each cartridge and then a modem in the cartridge reader can be used to transmit the votes over telephone lines. The cartridge reader can also print out a results tape of all votes cast in a precinct.<sup>99</sup> The total tape and cartridges can then become part of the official record of the election.<sup>100</sup>

### What to Look For

- **Security Seals.** Ideally, the Advantage’s exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this:

---

<sup>95</sup> The color of the voting ticket is used to specify the precinct or party (in a partisan primary) for which the voter is permitted to cast votes. For a particular ballot style, voters cannot vote for a race or party in which they are not allowed to vote (the choices for those races are disabled and cannot be selected).

<sup>96</sup> This can depend on local election law, procedures and regulations.

<sup>97</sup> This is Random Access Memory (RAM) and needs electricity – from a battery – to keep votes in storage. An event log, maintenance log and audit log is also stored on the memory pack.

<sup>98</sup> Specifically, the AVC Advantage’s interface is a switch matrix. That is, the screen can be thought of as a grid with rows and columns and it is the grid position of each choice that is recorded for each race. The votes are stored as strings (ASCII characters; for example, “A9,B2,...”).

<sup>99</sup> Printing the results before connecting the modem is preferable.

<sup>100</sup> Vote records can be re-read off of the redundant memory in the Advantage if a cartridge fails.



## Electronic Voting Machine Information Sheet

<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.

- Broken buttons, broken lights. As mentioned above the Advantage is a “button-matrix” DRE where the voter presses a button over which the machine’s paper ballot face is placed (under a plastic cover). A light lights up next to each selection by the voter. These buttons and lights, especially the frequently used ones in Federal races, can break or burn-out. If you see evidence of this – e.g., a light not lighting up after multiple button presses – you should request that the machine be pulled from service or that the button in question be serviced.
- Fleeing voters/premature voting. Some voters can be easily confused in that they press the vote button too early or not at all. If a voter complains that they only were able to vote on the first few races, they probably pressed the vote button before they were finished voting their ballot. Unfortunately, there’s not much to be done here other than emphasize that voters should make sure that they press the vote button *only after* they are certain they have voted as they want to in all races on the ballot. If a voter neglects to press the vote button and leaves a valid ballot on the machine, poll workers will probably have procedures to deal with this problem. We recommend that a poll worker reach in between the curtains and simply cast this vote.
- Incorrect ballot style. The Advantage can accommodate a number of different ballots, for different precincts, by disallowing voters to vote in contests for which they are not eligible. If a voter complains that their party (in a primary) races are not activated or that local races specific to their precinct are not activated, the poll worker probably pushed the incorrect ballot style option. The poll worker should cancel that ballot and activate the correct one.
- Incorrect Totals Tapes. The Advantage has been shown to incorrectly add up the number of voters given a particular ballot style when compared to the number of votes cast.
- Sensitive Disability Access Panel. The disability access panel on the Advantage is particularly sensitive. Viruses and other malicious programs, including some that could change vote data, could easily be introduced through the ADA accessibility interface. The flash memory used for audio files to accommodate voters with visual impairment should be sealed with tamper-evident seals and monitored at all times.
- Misleading Activation. When the Advantage is not activated to vote a valid ballot, it will still go through the motions in a way that will confuse voters into thinking that they ballot was cast. It even goes as far as to say, “Vote recorded -- thank you!”, despite the fact that it couldn’t have recorded the ballot since it was not activated to do so.



## Electronic Voting Machine Information Sheet

### Past Problems

**October 2008:** *New Jersey.* Princeton University computer scientists publish a court-ordered review which questions the accuracy and security of the Advantage.<sup>101</sup> Even when not properly activated, the Advantage will still indicate to voters that they have voted.<sup>102</sup> Vote-switching software could be installed in a single unattended machine and spread throughout a county's stock of voting machines.<sup>103</sup> The Advantage is associated with a high undervote rate for public measures.<sup>104</sup> Since the publication of the report, Union County, NJ's election official has encouraged voters to vote absentee by paper ballot rather than use the Advantage.<sup>105</sup>

**February 2008:** *New Jersey.* Programming errors cause Advantage machines in 8 New Jersey counties to report inconsistent Presidential primary results in their internal memory and removable memory storage. Programming errors caused some voters to be disenfranchised.<sup>106</sup>

**May 2006:** *New Jersey.* Questions about how many voters participated in the May 2 elections caused several candidates to question results regarding runoffs and vote counts. The Trenton City Clerk said he had contacted the vendor, Sequoia some two months prior but had not heard back.<sup>107</sup>

**November 2004:** *Louisiana.* State election officials received about 200 complaints of problems with machines, including two confirmed reports of Sequoia AVC Advantage voting machines in New Orleans Parish that were not working, according to Scott Madere, press secretary for the Louisiana Secretary of State.<sup>108</sup>

**November 2004:** *New Mexico.* Presidential undervote rates (ballots without a vote for president) were greater for ballots cast on the Advantage than those cast on any other type of system used on Election Day. One in every 19 ballots cast on Advantage machines did not register a vote for president.<sup>109</sup>

---

<sup>101</sup> "Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine," Andrew W. Appel and colleagues, <http://cobnitz.codeen.org/citp.princeton.edu/voting/advantage/advantage-insecurities-redacted.pdf>

<sup>102</sup> Id., p.81

<sup>103</sup> Id., p. 64

<sup>104</sup> Id., p. 85

<sup>105</sup> "Union County clerk says voting machines are unreliable; encourages voting by mail,"

NJPoliticker.com, October 21, 2008, <http://www.politickernj.com/matt-friedman/24666/union-county-clerk-says-voting-machines-are-unreliable-encourages-voting-mail>

<sup>106</sup> "Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine," p. 117.

<sup>107</sup> Id.

<sup>108</sup> Id.

<sup>109</sup> Id.



## Electronic Voting Machine Information Sheet

### Sequoia Voting Systems AVC Edge

**Name / Model:** AVC / Edge<sup>110</sup>

**Vendor:** Sequoia Voting Systems, Inc.

**Voter-Verifiable Paper Trail Capability:** Yes.<sup>111</sup>



**Brief Description:** The Sequoia AVC Edge is a touch screen direct-recording electronic (DRE) voting machine. It is a multilingual voting system activated by a smart card that records votes on internal flash memory. Voters insert a "smart-card" into the machine and then make their choices by touching an area on a computer screen, much in the same way that modern ATMs work. The votes are then recorded to internal electronic flash memory. When polls close, the votes for a particular machine are written to a "PCMCIA card" which are removed from the system and either physically transported to election headquarters or their contents transmitted via computer network.

**Checking the Voter-Verifiable Paper Trail:** The Edge's optional voter-verifiable paper-trail printer is called the VeriVote. The VeriVote printer is a cash-register type printer and is located to the left of the touch screen. Jurisdictions using the Edge that do not use the VeriVote attachment include: the state of Louisiana.

**Detailed Voting Process:** When the voter enters the precinct, he or she is given a "smart-card" by a poll worker after confirming the voter is registered. A "smart-card" is a card the size and shape of a credit-card which contains a computer chip, some memory and possibly basic data such as the voter's political party. The voter then takes the smartcard to a voting machine and inserts the smart-card into the yellow slot visible in the middle picture above. The first screen presented to the voter is one that allows him or her to choose the ballot language. After using the touchscreen to vote, 1) the record of the vote is directly recorded electronically to two flash memory cards and 2) the voter's smart

<sup>110</sup> See: <http://www.sequoiavote.com/productguide.php?product=AVC%20Edge>

<sup>111</sup> When equipped with a VeriVote printer.



## Electronic Voting Machine Information Sheet

card is reset to ensure that the voter can only vote once. The AVC Edge may also be equipped in some precincts to print a voter-verifiable paper audit trail using the VeriVote printer. In this case, the voter will inspect the printout that is displayed underneath glass. If the paper accurately reflects the vote, the voter indicates so using the touchscreen and casts the vote; the printed paper is withdrawn into the machine to protect privacy. If the paper is incorrect, the voter may mark it as spoiled and change his or her vote using the touchscreen interface. After the vote is cast, the smart-card pops out of the machine and the voter returns it to a poll worker.

When the polls close, a poll worker or election official inserts a different-type of smart card, an administrator card, into each voting machine and puts the machine into a postelection mode where it will no longer record votes. At this point, the machine writes the votes from its internal memory to flash memory on a "PCMCIA card." The PCMCIA card is merely a removable form of flash memory. A printed tape of all votes cast or vote totals for the voting machine can also be printed out at this time depending on local procedure and regulations.

The PCMCIA cards are removed from each machine and either taken to a central tabulation facility or to remote tabulation facilities. At the tabulation facility the votes are copied from the PCMCIA cards and into a central computer database where precincts are combined to result in an aggregate vote. The votes may also be transmitted to the central tabulation facility via a closed "Intranet", the Internet or modem. The PCMCIA cards and possible any printouts from the voting machines can then become part of the official record of the election.

### Things to Look Out For

- **Security Seals.** Ideally, the Edge's exposed ports, memory card access areas and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this:  
<http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Memory Cards and Physical Access.** The internal (cryptographic) keys used to protect the Edge from software modification are hard-coded into the software. This means that physical access to a single Edge or Edge memory card could jeopardize the security of all Edge machines with a given hard-coded key. With this key, an attacker could forge a software update cartridge and upload software of her own design. Memory cards and physical access to Edge machines are sensitive and care should be exercised in terms of allowing unsupervised access to memory cards or Edge DRE units.



## Electronic Voting Machine Information Sheet

- **Poor Provisional Ballot Notification.** If a jurisdiction is using its Edges to allow electronic provisional votes, the only indication that a voter is casting a provisional vote with a provisional vote smartcard is the words “Provisional Voter” on the VVPAT tape. We are uncertain if there is any indication of provisional ballot status on Edge machines that do not use the VeriVote VVPAT attachment.
- **Forging and Duplication of Voter Cards.** With knowledge of the hard-coded key used with Voter Cards, it is possible to forge valid Voter Cards. Also, between the time a voter’s Voter Card is activated by the pollworker and used, it can be duplicated and used to vote multiple times, without any knowledge of the hard-coded key. Smartcard duplication equipment can be hidden easily on a voter’s person. To protect against duplicate voting, be on the watch out for some sounds that might indicate duplicate voting: 1) each time a Voter Card is ejected from the Edge, it makes a loud click sound; 2) also, if the Edge is equipped with the VeriVote VVPAT printer, printing out of the VVPAT record will also be noticeably loud each time a vote is cast.

## Past Problems

**August 2007: California.** Following an expert top-to-bottom review of voting systems which finds critical security vulnerabilities in the Edge, the Secretary of State disallows the machine’s use as a primary voting system.<sup>112</sup>

**March 2006: Florida.** Touch screen voting machines malfunction, switch votes on the screen. One candidate watched his vote for himself switch to his opponent.<sup>113</sup> Group calls for audit of March 7 elections. Members say the results are “highly suspect” after an elections staffer was given the code to a computer server.<sup>114</sup>

**November 2004: Washington.** Voters in at least four polling precincts in Snohomish County said they have encountered problems with the Sequoia electronic voting machines. When they touched the screen to vote for a candidate, an indicator showed they had selected the opposing candidate. It took at least four attempts before the indicator showed the correct candidate.<sup>115</sup>

**October 2004: New Mexico.** Votes change on the screen and are resistant to voter’s attempt to vote for their choice.<sup>116</sup>

---

<sup>112</sup> Sequoia Voting Systems, Withdrawal of Approval/Conditional Reapproval, Secretary of State of California, October 25, 2007, [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/sequoia\\_102507.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia_102507.pdf)

<sup>113</sup> Id.

<sup>114</sup> Id.

<sup>115</sup> Id.

<sup>116</sup> Id.



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## Electronic Voting Machine Information Sheet

**September 2004:** *Florida.* High percentages of undervotes in the primary election present the county with an unanswerable question since the paperless machines provide no method of doing an audit.<sup>117</sup>

### References:

“DRE Security Assessment, Volume 1, Computerized Voting Systems, Summary of Findings and Recommendations,” InfoSENTRY, 21 Nov. 2003. See:  
<http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf>

“Direct Recording Electronic (DRE) Technical Security Assessment Report,” Compuware Corporation, 21 Nov. 2003. See:  
<http://www.sos.state.oh.us/sos/hava/files/compuware.pdf>

---

<sup>117</sup> See <http://www.votersunite.org/info/Sequoiaintheneeds.pdf>



**Electronic Voting Machine Information Sheet**  
**Sequoia Voting Systems Optech III-P Eagle**  
**(also ES&S Optech III-P Eagle)**

**Name/Model:** Optech III-P Eagle

**Maker:** Sequoia Voting Systems

**Voter-Verified Paper Record Capability:** Uses paper ballots



**Brief Description:** As an optical ballot tabulator, the Optech III-P Eagle functions at the precinct level. The Optech III-Eagle consists of an electronic ballot counting device which reads completed ballots by scanning for the voters' marks indicating their voting preferences. The Optech III-Eagle then tabulates the results. When the polls close, the results are both printed on a paper copy and stored to an internal memory card.<sup>118</sup>

The Optech III-Eagle runs off both internal and external power to reduce the risk of malfunctions, and it can store voter data on an internal memory card, transmit data via phone lines or satellite, and it can print out paper copies of voter results.

**Detailed Voting Procedure:** The Optech III-Eagle functions much like a traditional paper ballot system. Upon entering the voting precinct, the voter will receive a paper ballot; the voter shades in the paper ballot with any standard pen or pencil and inserts the ballot into the Optech III-Eagle, which then ensures that the ballot has been properly marked and that no over or under voting has occurred. As votes are entered, the Optech III-Eagle stores the vote tallies on its internal memory card., and when the polls close, the Optech III-Eagle prints out a paper copy of the election results for polling officials.<sup>119</sup>

<sup>118</sup> From the manufacturer's website, available at: <http://www.sequoiavote.com/bEAGLE.php>

<sup>119</sup> From the manufacturer's website, available at: <http://www.sequoiavote.com/bEAGLE.php>



## Electronic Voting Machine Information Sheet

### What to Look For

- **Security Seals.** Ideally, the Eagle's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should be locked and/or be sealed with tamper-evident tape.
- **Keys.** The keys for the Optech III-P Eagle are the same for all Optech III-P Eagle machines and are easily pickable with readily available tools. Care should be observed around the ballot box lock and the scanner key lock (turns the system off and on).
- **The Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **Correct Inks.** Some models of the Eagle have trouble reading red inks or inks with red in them. These Eagles use an infrared lamp to detect voting marks and red or reddish inks appear "blank" under this light. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.

### Past Problems:

There have been some reported problems with the Optech III-Eagle, although not as many as with other systems, although this may be because of the relative newness of the system. One known issue is that there can be compatibility problems between the Optech III-Eagle and other Sequoia Voting Systems, such problems having led to tabulation delays and errors in multiple cities in the Wisconsin primary elections in 2006.<sup>120</sup>

---

<sup>120</sup> Compiled from various news reports, from the VoteTrustUSA website, available at: [http://www.votetrustusa.org/index.php?option=com\\_content&task=view&id=1793&Itemid=113](http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1793&Itemid=113)



## Electronic Voting Machine Information Sheet

### Sequoia Optech Insight

**Name/Model:** Optech Insight and Optech Insight Plus

**Maker:** Sequoia Voting Systems

**Voter-Verified Paper Record Capability:** Uses paper ballots



[photo obtained from: [http://www.michigan.gov/images/sos/pic04a\\_225434\\_7.JPG](http://www.michigan.gov/images/sos/pic04a_225434_7.JPG)]

**Brief Description:** This information sheet describes both the Optech Insight and the Optech Insight Plus as “the Insight.” Both are optical scan machines which are used to read and tabulate ballots at the polling place. According to the California Secretary of State’s 2007 Top-to-Bottom Review of voting systems, the major difference between the Insight and the Insight Plus seems to be that the Insight Plus has an LCD screen for displaying messages to voters. On both models, there is also a small four-digit LED screen that shows how many ballots have been accepted since the polls opened.<sup>121</sup>

The Optech Insight consists of an electronic ballot counting device which reads completed ballots by scanning for the voters’ marks indicating their preferences. The scanner sits atop a ballot box. The Optech Insight then tabulates the results. When the polls close, the results are both printed on a paper copy and stored to an internal memory card.

---

<sup>121</sup>Source Code Review of the Sequoia Voting System. Secretary of State of California’s Top-to-Bottom Review of Voting Systems, August 2007, p.16. Available at: [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/sequoia-source-public-jul26.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf)



## Electronic Voting Machine Information Sheet

The Optech Insight runs off both internal and external power to reduce the risk of malfunctions, and it can store voter data on an internal memory card.

**Voting on the Optech Insight and Insight Plus:** Upon entering the polling place, the voter will receive a paper ballot. The voter makes choices on her ballot by connecting an arrow next to her choice of candidate or issue position. The voter inserts the ballot into the scanner at the top of the device, which reads the marks on the ballot. If the voter has overvoted (voted for more candidates than eligible), the Insight will eject the ballot for the voter to review again, or deposit the ballot into the ballot box. If the voter has cast a write-in vote, the scanner will feed the ballot into a center bin so that poll workers may process the write-in votes. Ballots that require no review by poll workers are deposited into a rear bin. A front, auxiliary bin is available in case the machine is not functioning during polling hours; voters deposit ballots into the auxiliary bin manually, but they will not be able to use the auxiliary bin unless poll workers have unlocked it.

As votes are entered, the Optech Insight stores the vote tallies on its internal memory card., and when the polls close, the Optech Insight prints out a paper copy of the election results for polling officials.<sup>122</sup>

The Insight has an optional modem for transmitting election results, and can also transmit results via a proprietary Sequoia device called a Hybrid Activator and Accumulator (HAAT). The HAAT accumulates results from machines in a polling place, and transmits them to the jurisdiction's central election office via a wireless cellular network.<sup>123</sup>

### What to Look For

- **Security Seals.** Ideally, the Insight's exposed ports, memory card access areas, ballot box doors and case seams would be covered with tamper-evident security seals. The integrity of these seals should be maintained at all times, and only breached under controlled, explained circumstances. A voided seal looks like this: <http://www.flickr.com/photos/joebeone/2247733620/> . Seals should be logged to maintain chain of custody of sensitive materials.
- **Ballot Box Access.** Optical scan systems have at least one and possible more ballot boxes. Each ballot box should be inspected by a voter at the beginning of voting to make sure that they are empty. These ballot boxes should locked and/or be sealed with tamper-evident tape.

---

<sup>122</sup> From the manufacturer's website, available at: <http://www.sequoiavote.com/bEAGLE.php>

<sup>123</sup> Source Code Review of the Sequoia Voting System. Secretary of State of California's Top-to-Bottom Review of Voting Systems, August 2007, p.10. Available at: [http://www.sos.ca.gov/elections/voting\\_systems/ttbr/sequoia-source-public-jul26.pdf](http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf)



**ELECTION PROTECTION** **YOU HAVE THE RIGHT TO VOTE**  
**1-866-OUR-VOTE**

## **Electronic Voting Machine Information Sheet**

- **Keys.** The keys for the Insight and Insight Plus models are the same for all machines and are easily pickable with readily available tools. Care should be observed around the ballot box lock and the scanner key lock (turns the system off and on).
- **The Removable Memory Card is Sensitive.** Corrupt memory cards may be able to introduce viruses, cause the main election server to crash and falsify votes. Access to the memory card should be controlled, monitored and logged at all times.
- **The System Chip is very sensitive.** The main software chip on the Insight, the HPX chip, is easily replaceable with minimal access to an Insight scanner. A malicious HPX chip could count votes incorrectly, selectively accept or reject ballots and ignore system software updates.
- **Correct Inks.** Some models of the Optical Scan systems have trouble reading red inks or inks with red in them. Voters should use the writing instrument provided at the polling place or, if voting at home, a black ballpoint pen that does not bleed through paper.