# Critical Elements In Enhancing Accuracy, Security and Accessibility of DRE with VVPB and Electronic Optical Scan with VMPB in Recording Voter Intents

AVANTE International Technology, Inc.
70 Washington Road, Princeton Junction, NJ 08550
www.vote-trakker.com avante@aitechnology.com

## State of Our Election Counting Systems

Direct recording electronic (DRE) with and without voter verified paper ballots (VVPB) or voter verified paper audit trail (VVPAT)[1] have been roundly criticized and in some circles feared for their potential errors and proven problems. Undeniably, the earlier generations of DRE lacked independent verification, they also had inadequate engineering and technical design for reliability and system security. The engineering and technical flaws[2] caused dramatic failures in multiple elections. Florida [3] [4] (Sarasota County) has become a lightning rod symbolizing electronic voting woes. Adding to the problems, most DRE systems implemented with VVPB or VVPAT were done by vendors that have been fighting against them. They also failed spectacularly. The glaring and disturbing failures of DREs with VVPAT that happened in the Primary Election in Ohio in 2006 [5] are one of the best examples of problems caused by inadequate engineering. Is DRE voting, even with voter verified paper ballots, really the wrong solution? Or, is it the poor design and engineering used in DRE with VVPB the real problem?

Some of the citizens and voting integrity watchdog groups along with some computer scientists are now calling for the use of paper ballots counted with optical scanning technology as the "right" solution. The advancing argument is that with voter marked paper ballots, one can always trace back to the original votes as cast. However, one cannot stop wondering what security, accuracy, and reliability problems will we discover on these electronic optical scan systems if we put the same amount of scrutiny that we used on DREs. After all, if we cannot trust electronics that record votes verified by voters on the voting machine screen and on its corresponding paper record, how can we really trust electronic systems that scan and tabulate paper ballots without telling the voters how the paper ballots are being deciphered beyond whether there may be over-votes or under-votes?

As the company that pioneered the voter verified paper ballot for direct recording electronic, and the optical scanning electronic voting solution that can authenticate the paper ballots, and captures the ballot images as audit trail, in this shortened version of a full white paper [6], AVANTE will relate our experience in solving these problems. We will also detail the best technical solutions from a manufacturer and solution provider's perspective.

## Is An Electronic Optical Scan Voting System Any More Secure Than DRE with VVPB?

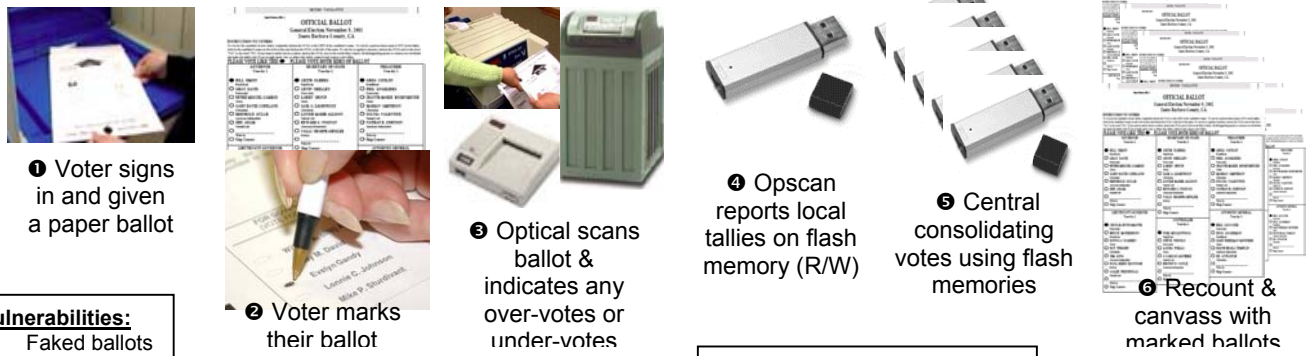
The precinct-based optical scan voting system certified for use by most states, uses 20 years or older discrete sensor scanning technology to read the marked ballots and uses computer and electronics for tabulation. They inevitably inherit the same computer-related security vulnerabilities like those associated with DREs. It has been documented that they read and/or record the ballot incorrectly because of imperfect software and hardware. Because of less attention paid to securing these systems, the nature and the extent of these vulnerabilities may be even more critical.

---

[1] In this discussion, we refer the to the voter verified paper records as VVPB if such paper records are the official ballot, and VVPAT when electronic votes rather than paper records are the controlling vote data.
[2] "THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST"; THE BRENNAN CENTER FOR JUSTICE; http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf
[3] Sarasota Officials Freeze Election Data, as Jennings Battle Wages On; http://www.nytimes.com/cq/2007/02/02/cq_2229.html
[4] "Factors Associated with the Excessive CD-13 Undervote in the 2006 General Election in Sarasota County, Florida"; Walter R. Mebane, Jr. David L. Dill http://www.votetrustusa.org/pdfs/Florida_Folder/smachines1.pdf
[5] DRE Analysis for May 2006 Primary Cuyahoga County, Ohio http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf
[6] http://www.vote-trakker.com/White%20Papers/PAPER%20SCANNING%20VS%20ELECTRONIC%20BALLOT%20WITH%20VOTER%20VERIFIED%20PAPER%20BALLOT.pdf

Figure 1 below represents the process of a typical precinct-based optical scanning (PBOS) voting system (commonly referred to as Opscan). There are two facets of this voting system that may not have been clearly delineated because of confusing terminology. The term "optical scan voting system" seems to ignore that it's the electronics and computer that actually drive the critical reading and counting function of the system. The second facet is that PBOS or Opscan is also a direct recording electronic (DRE) voting system! Instead voters make selections on a touch-screen, the voters make selections by marking on the paper ballot (VMPB). Once the ballot is submitted, it records the votes to provide the tallies. Like VVPB, VMPB are stored and used for audit. Based on the above description, a more descriptive name will be "Precinct-Based **Direct Recording Optical Scanning Electronic (DROSE)** voting System".

The depictions under Figure 1 represent today's precinct-based DROSE system with the well-known vulnerabilities [7] [8]. The data transfer media uses flash memories that lack adequate security and can be changed without leaving a trace. With the use of paper ballot, the inherent vulnerability to counterfeiting, tampering via smearing, changing, substituting, adding and removing of paper ballots are well documented over the last 100 years and more. [9] [10] [11]



❶ Voter signs in and given a paper ballot

❷ Voter marks their ballot

❸ Optical scans ballot & indicates any over-votes or under-votes

❹ Opscan reports local tallies on flash memory (R/W)

❺ Central consolidating votes using flash memories

❻ Recount & canvass with marked ballots

**Vulnerabilities:**
- Faked ballots are readily made.
- Chain-of-custody on blank ballots are difficult to keep without errors.
- Costly to print and manage hundreds and thousands of different ballot styles in a polling place.

**Vulnerabilities:**
- Voters are known to make 1.5% under and over votes and other errors for the critical presidential race.
- Error rates increase to 3.5-20% for other lesser races.

**Vulnerabilities:**
- Ballots are scanned and counted electronically with up to 0.5% error inherently.
- DROSE only tells you that you have some "over-voted" or "under-voted" contests but NOT how your vote is read and counted!
- There is no indication that your vote is counted and counted correctly.

**Vulnerabilities:**
- All systems today use read/write flash memories to transfer vote tallies.
- Flash memories can be changed without a trace..
- No images of the paper ballots as scanned are captured or available.
- If the retained paper ballots are erased, smeared, tampered, or substituted, no evidence can be traced.
- That is, all is well when the tampered tallies "matches" the tampered paper ballots to within 0.5-2.0%!

**Vulnerabilities:**
- Since no images of ballots are kept, as long as the flash memories are changed to match that of the erased, smeared, substituted paper ballots, it is not traceable. .
- Of course with the "no fault" absentee voting, there are plenty of paper ballots that can be added or played with.

Figure 1: Direct recording optical scanning electronic paper ballot system and inherent vulnerabilities.

It may be surprising to many that none of the vulnerabilities related to the use of paper ballots have been addressed by the DROSE systems deployed today.

[7] Election Administration in the United States. Brookings; Joseph Harris. 1934; http://vote.nist.gov/electi admin.htm
[8] "Accuracy, Integrity, and Security in Computerized Vote-Tallying", Saltman, Roy G. 1988; http://www.itl.nist.gov/lab/specpubs/500-158.htm
[9] "ANNALS OF DEMOCRACY COUNTING VOTES" By Ronnie Dugger; The New Yorker, November 7, 1988
[10] "Computerized Voting. Evaluating the Threat..." Proc. Third ACM Conf. on Computers, Freedom & Privacy. San Francisco, CA (Mar. 1993); Shamos, http://www.cpsr.org/conferences/cfp93/shamos.html
[11] "Computerized Systems for Voting Seen as Vulnerable to Tampering"; By D. BURNHAM; The New York Times; July 29, 1985 http://www.newsgarden.org/columns/burnham1.shtml

Is there a real technical difference between DRE with VVPB and DROSE with VMPB? What is a "Ballot Marking Device"? How does it provide accessibilities for paper ballots?

In the case of DRE with VVPB, the properly designed machine "guides" the voters to make the selections and prints out a paper ballot for the voter to verify and stores the VVPB for audit. In the case of DROSE, the system deciphers the VMPB and informs the voters of any under-voted or over-voted contests but not how the ballot is actually going to be recorded. Once the voter presses the cast ballot button, the VMPB is dropped into a storage bin as a record. In the case of a "ballot marking device" (BMD), instead of recording the vote directly, the BMD perform the same tasks of "guiding" the voter to make selections, marks/prints the paper ballot and lets the voters submit their ballots manually.[12] [13] If one simply opens the case shielding the VVPB of the DRE system and allow the voters to submit their VVPB manually, the only technical difference is whether what is recorded in DRE is used as an audit or as actual votes.[14] It is obvious that both DRE and BMD can and have incorporated voice-assistance and read back for visually impaired, and binary switches for voters with dexterity issues, to provide HAVA mandated accessibility provisions. It is technically impossible to provide "true independent accessibility" to the visually impaired voter for both VVPB and VMPB from any vendors. AVANTE has detailed the technical considerations and suggested that the EAC or other public organizations develop a free module based on a 2-D barcode, to provide such facilities in a separate white paper.[15]

**How can we buttress the security and minimize the vulnerabilities of paper balloting in general, and "Direct Recording Optical Scanning Electronic" voting system in particular?**

All of the currently available precinct-based DROSE systems have high incidences of voter errors and the potential for insider hacking and tampering. One of these vulnerabilities has been demonstrated in "Hacking Democracy" by Bev Harris and associates.[16] Bev Harris and associates with "Black Box Voting" besides demonstrating the vulnerabilities of the DROSE, have also proposed two solutions that AVANTE believes to be technically correct:

1. Hand counting of ballots under public supervision at the precinct after the poll is closed[17]. While this method cannot resolve voter errors of under and over votes, it offers the security of audited tallies. It defeats any attempts to tamper with the counted ballots and adding new ballots. There are still other technical problems that need addressing:
   - Marginal markings on ballots will make finishing counting difficult in close elections.
   - It is difficult for humans to distinguish well-printed fake ballots if they are injected.
   - Most US elections have 10-50 contests with tens to hundreds of candidates. Unless we limit the number of contests, hand counting could take hours if not days to finish.
2. Use a DROSE that captures the ballot images as cast and posts/publishes the ballot images for the public to verify the tabulated results[18]. It will be obvious that this solution is more useful when the ballot images are captured in real-time at the precinct. The same applies for the central office when processing absentee ballots. It will be even better if the paper ballots can be authenticated individually without causing privacy concerns.

---

[12] US Patent 6,892,944 Electronic voting apparatus and method for optically scanned ballot

[13] US Patent 7,080,779 Ballot marking system and apparatus

[14] "A Manufacturer's View Point On the Voter Verifiable Paper Record and Audit Trail" http://www.vote-trakker.com/White%20Papers/A%20Manufacturer%27s%20View%20Point%20On%20the%20voter%20verifiable%20paper%20record%20FINAL.pdf

[15] Accessibilities of "voter verified paper ballot" to visually impaired voters http://www.vote-trakker.com/White%20Papers/Accessibilities%20of%20VVPB-RUNYAN.pdf

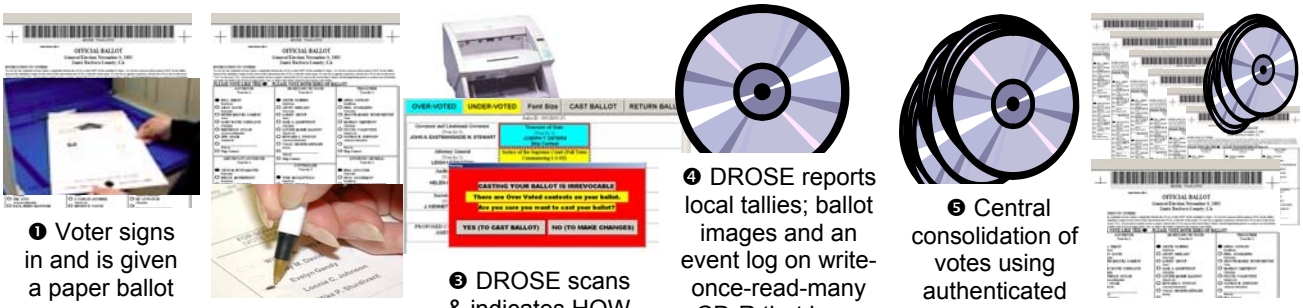
[16] http://www.blackboxvoting.org/BBVreport.pdf

[17] http://www.bbvforums.org/forums/messages/1954/40411.html?1159836941 http://www.bbvforums.org/forums/messages/157/were_counting_the_votes_2006_09_02-40394.pdf

[18] Harri Hursti's invention, http://www.bbvforums.org/forums/messages/1954/10268.html

Figure 2 below represents a solution[19] designed to address most of the inherent vulnerabilities when using paper ballots in the precinct-based DROSE system. The following are some of the enabling improvements over the traditional DROSE systems:

1. Include a method to help reject fake and counterfeit ballots and prevent double counting of any paper ballots. The proposed method includes the use of machine-readable, (e.g. barcode) randomly generated, and a unique ballot identifier.
2. Tell the voter exactly how the voting system is reading the VMPB. That is, the system should inform the voters beyond, whether there are over-voted or under-voted contests.
3. Capture scanned ballot images to provide electronic audits to prevent post-election ballot switching, smearing, ballot loss and other tampering. Use of write-once-read-many CD-R or DVD that are countersigned by the poll workers to provide an irrefutable audit trail for the images and tallies of the paper ballots.



❶ Voter signs in and is given a paper ballot

❷ Voter marks their ballot

❸ DROSE scans & indicates HOW the ballot is deciphered and any over or under votes. DROSE also captures the ballot images.

❹ DROSE reports local tallies; ballot images and an event log on write-once-read-many CD-R that have been authenticated by the jurisdiction and "signed" by precinct election officials and/or observers.

❺ Central consolidation of votes using authenticated and signed WORM CD-R instead of flash memories.

❻ Recount & canvass with marked ballots and/or WORM CD-R that can be authenticated.

**Vulnerabilities Mitigated:**

- Ballots bearing machine-readable unique random identifier **cannot be faked or duplicated**.
- Unlimited number of ballot styles can be printed at the polling places on-demand.
- In response to the concern based on "privacy", one should point out that a machine-readable authentication identifier is a far less problem than "no fault" absentee

**Vulnerabilities Mitigated:**

- Ballots are scanned and **imaged** as audit trail.
- DROSE should **display exactly how your ballot is read and counted** along with any "over-voted" or "under-voted" contests.
- It still cannot help you to correct the errors without submitting a new ballot.
- **Pixel measurement resolves lighter marking.**

**Vulnerabilities Mitigated:**

- Since real-time ballot images are kept, any subsequently submitted and tampered paper ballots for DROSE can be easily traced.
- The use of **signed WORM CD-R as transfer media and the inclusion of ballot images and an event log makes insider tampering almost impossible without being caught.**
- This solution cannot resolve the potential adding, substituting, tampering of absentee paper ballots.

Figure 2: Direct Recording optical scanning electronic system with imaging capabilities to provide electronic audit.

## How should one buttress the security of DRE with voter verified paper ballot?

Even though paper balloting with precinct-based optical scanning electronic systems can be dramatically improved, as illustrated in Figure 2 above, there are several inherent problems that cannot be addressed even with the best of technologies:

- The system can only remind the voters of mistakes but cannot help the voters to correct the errors directly. Voters must take the initiative to do it over. It has been documented that 75% of these voters who are give the chance to make corrections will not bother with the trouble of having to get a new ballot and do the paper ballot over. Properly

[19] OPTICAL VOTE-TRAKKER™: A "Mark-Sense" Absentee & Precinct Based Voting System that Minimizes Both Voter and System Errors http://www.vote-trakker.com/OpticalVote-Trakker.pdf

engineered DRE with VVPB "guides" the voters in avoiding all errors for a true 100% accurate reflection of voter intent [20].

- Paper ballot systems are incapable of providing accessibility to some voters with visual or dexterity disabilities. Separate accessible solutions such as ballot marking devices or direct recording electronic voting systems must be provided. This makes pollsite management more complex.
- Only a DRE with VVPB that can be authenticated against loss and tampering, allows all voters to vote on the same system. It is equitable and democratic.

Figure 3 below is an illustration of a properly designed DRE with VVPB that solves all of the known problems of the earlier generation systems. These solutions are not only possible but built and proven by AVANTE.

❶ Voter signs in and is given a ballot access card that is secured against counterfeiting. Alternatively, pollworkers control access.

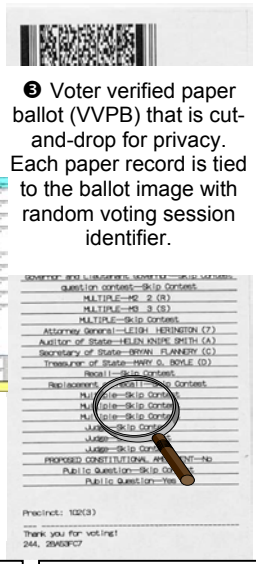
**Vulnerabilities Mitigated:**

- Use of unique random identifier eliminates counterfeiting.
- Use orientation independent ballot access card to ease system failure and extra accessibility for the voters with disabilities.

❷ Voter is "guided" through one-contest at a time for paging screen or pro-active warning and requiring positive acknowledgement of under votes on full-face ballot.

**Vulnerabilities Mitigated:**

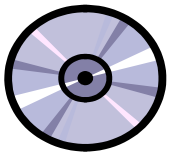
- 0% over vote.
- **One contest per screen for paging** DRE with VVPB and innovative **use of "Skip Contest" to eliminate all unintentional under votes.**
- Proper engineering of touch-screen to ensure lifetime calibration stability for the paging DRE with VVPB.
- Use of better touch-screen technologies to ensure accuracy and stability for the touch-screen DRE with VVPB.



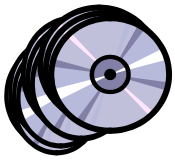
❸ Voter verified paper ballot (VVPB) that is cut-and-drop for privacy. Each paper record is tied to the ballot image with random voting session identifier.

**Vulnerabilities Mitigated:**

- Cut-and-drop VVPB paper record to ensure privacy.
- Use at least 800-ft of paper or at least double the normal usage to ensure system availability.
- **Automatic system shutdown whenever VVPB printer is not functioning.**
- Use archive grade thermal paper to ensure stability.
- VVPB is tied to individual electronic ballot image protecting system against insider tampering.



❹ All DRE with VVPB should use write-once-read-many CD-R that is authenticated by the jurisdiction and signed by pollworkers as transfer media to prevent tampering.



❺ Central consolidation of votes uses WORM CD-R to ensure end-to-end system integrity.

❻ Recount & canvass with VVPB and/or authenticated CD-R.

**Vulnerabilities Mitigated:**

- WORM **CD-R authenticated by the jurisdiction and signed by the pollworker, eliminates any insider and outsider tampering.**
- CD-R has adequate capacity to include all ballot images, event log, and local tallies.
- **Linking each VVPB with electronic ballot images with random voting session identifier enables end-to-end auditing.**
- 100% availability of high quality and individual VVPB enable verification of system integrity.
- A properly designed/engineered DRE with VVPB is the only method to provide both accessibility and elimination of all voter errors.

Figure 3: Examples and illustration of DRE with VVPB that have been proven to be reliable and secure.

The following are the improvements that have been incorporated in a properly designed DRE with VVPB based on EAC 2005 Voluntary Voting System Standards:

1. Only New York and Illinois State Election Codes ask for the right VVPB for DRE voting systems. Each and every voter verified paper ballot is linked one-to-one to a corresponding

[20] SUMMARY OF EXPERIENCE: AVANTE ELECTRONIC VOTING MACHINES http://www.vote-trakker.com/White%20Papers/accolade-%20Summary%20of%20experience%20Nov.%203,%202003%20election.pdf

electronic vote to provide end-to-end auditing as required in the EAC 2005 VVSG. The rest of the 25 of the 27 states requiring DREs to incorporate VVPB or VVPAT have been misguided to ask for inferior solutions. In the case of DRE with VVPB used in Ohio that "miss printing" or "fouled up" close to 10% of the VVPB, the damage to voter confidence would have been minimal if there was one-to-one tracking between the electronic ballot images and VVPBs. Any one of the paper records can be authenticated with the corresponding electronic ballot images to project the accuracy of the rest of 10% of the VVPB. If the ballots lost are random, this cross check is equivalent to a 90% audit that will statistically discover almost any problems.

2. Properly designed voter interfaces for both paging and full-face DRE voting systems to prevent voter errors. Voter is "guided" through one-contest at a time via a paging screen with a choice of "Skip Contest" to ensure 100% reflection of voter's intent or 0% unintentional residual vote. In the case of full-face voting system, provide a pro-active warning and require a positive acknowledgement for those contests that are to be left under-voted.
3. Ensure all transfer media for election data (tallies, ballot images and event log) to be write-once-read-many media such as CD-R or DVD. Adopt procedure of having the pollworkers countersign the CD-R from each voting unit of DRE with VVPB and the same for DROSE. They are low cost and secure. If acceptable, post and publish all of the ballot images from the DROSE systems to provide the transparency that most election integrity groups look for. Voting systems using such media are available today for both DRE with VVPB and DROSE.

**Conclusion:**

Our complex society will likely require the use of both DREs with VVPB and optical paper ballot solutions to provide 100% accessibility to all voters for the foreseeable future. The nation will be best served for all of us to focus on all aspects of improvements for both systems. AVANTE has proven the security and reliability of properly designed and engineered DRE with VVPB. They help to guide voters to avoid all unintentional under-votes besides the prevention of over-votes.

The following are the critical missing links to enhance security and reliability of our nation's voting systems:

1. We endorse HR 811 of Congressman Holt in mandating all DRE voting systems without paper records to immediately be retrofitted with VVPB. To guard against tampering and loss of VVPB, every voter verified paper ballot must have one-to-one correspondance to the electronic vote to provide end-to-end auditing as described in the EAC 2005 VVSG.
2. If paper balloting is to be used more extensively than for limited absentee voting only, we should require paper balloting systems to have the same level of security and anti-counterfeiting as that of the best designed and engineered DRE with VVPB.
   - Incorporation of a machine-readable randomly generated ballot identifier will minimize vote tampering by the traditional "ballot stuffing", "ballot switching", "ballot loss", and "ballot modification" [21] [22] [23].
   - Require all optical scan systems to capture the images of the paper ballots in real-time as part of the audit trail. This measure reduces the need to have absolute chain-of-custody management in direct recording optical scanning electronic voting systems.
3. Demand all election data (tallies, ballot images, and event log) to be transferred with write-once-read-many media such as CD-R/DVD. They are low cost and secure against any post election tampering.

[21] Paper v. Electronic Voting Records – An Assessment Michael Ian Shamos; http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm
[22] The Election Integrity Audit; Kathy Dopp and Frank Stenger; http://electionarchive.org/ucvAnalysis/US/paper-audits/ElectionIntegrityAudit.pdf
[23] http://www.vote-trakker.com/White%20Papers/OPTICAL%20VOTE-TRAKKER%20MINIMIZING%20VOTERS%20AND%20SYSTEM%20ERRORS.pdf