

July 10, 2006



Verified Voting's Commentary on the June 2006 EAC Oversight Hearings

Verified Voting provides the following analysis and commentary regarding certain points made during the Election Assistance Commission (EAC) Oversight Hearing conducted in June 2006 by the congressional Committee on House Administration. We refer below to questions or comments the Committee members posed to the Commissioners, and their responses, during the hearing. Each section references comments transcribed from the video posted at the Committee's website¹ following the hearing (see attached Exhibit I).

SUPPORT FOR VOTER-VERIFIED PAPER RECORD² REQUIREMENTS

The Committee discussion noted the extensive support for voter-verified paper records.³ To date, 28 states have passed voter-verified paper record requirements, and another eight states⁴ are deploying voter-verifiable equipment statewide, through their recent HAVA purchases. Thus 36 states (over 70%) have concluded that voter-verifiable voting systems are necessary for trustworthy elections.

One Commissioner, commenting on this trend, asserted that states lacking VVPR requirements are content with the status quo. However, we believe it may not be the case that the remaining states have "chosen not to" implement VVPR because they "feel comfortable in the system that's set up," but rather that in several of those states, an ongoing struggle is taking place.⁵ The legislatures of several pivotal states have come very close to enacting VVPR requirements recently.⁶ That those bills have not yet passed has more to do with fiscal concerns or political maneuverings of a few powerful committee chairs rather than of the voters or a majority of the lawmakers in those states being comfortable with their current systems. In fact, most could be described as **un**comfortable.

Several bills⁷ in the U.S. House of Representatives would require voter-verified paper records (VVPR), of which H.R. 550 is the clear leader with 193 bi-partisan co-sponsors at this time, and by far the best bill. Without duplication, the combined co-sponsorship of the various pending VVPR bills shows that at this time, a majority of the members of the U.S. House of Representatives are on the record as supporting legislation to enact a requirement for VVPAT/VVPR for all voting systems used in federal elections.

DREs: TRUSTWORTHY WITHOUT VVPAT?

Simply put, paperless DREs cannot be made trustworthy. No paper trail printed post-election, without the benefit of voters confirming that the document represents their intent, can change that.

¹ <http://cha.house.gov/hearings/hearing.aspx?NewsID=1353>

² It is important to note that voter-verified paper records (VVPR) are not limited to voter-verified paper audit trails (VVPAT) attached to direct recording electronic (DRE) voting machines. The broader term includes paper ballot-based systems such as the precinct-count optical scan used in more jurisdictions nationwide than any other system. Paper ballots, marked by the voter, are inherently voter-verified.

³ Before 2000, NH and SD had statutes requiring paper ballots. IL, MI and NV passed voter-verified paper record requirements before the end of 2003. In 2004, AK, CA, ME, MO and OH added requirements, and NV became the first state to fully implement VVPAT with DREs. Details at: <http://verifiedvoting.org/article.php?list=type&type=13#state>.

⁴ AL, MA, MS, ND, NE, OK, RI, WY

⁵ Twelve states and the District of Columbia have introduced and/or are currently considering a VVPR requirement.

⁶ E.g. Maryland, where this year such legislation passed unanimously in one chamber but was denied a meaningful hearing in the other, despite urging by the Governor; Iowa, where the bill passed unanimously in one chamber but was attached to un-passable language in the other; Tennessee, where a legislative study committee is set to review the matter; Virginia, where strong bi-partisan bills were tabled due to budget issues, but not rejected.

⁷ <http://www.verifiedvoting.org/legis>

Security "start to finish" is a misnomer when jurisdictions buy systems already built. If faulty or malicious code resides in the system when they receive it, they won't know. Without the explicit requirement for voter-verified paper records and robust mandatory random manual audits of those records, the VVSG and Management Guidelines procedures to which the Commissioners refer cannot resolve an end-to-end security dilemma.

Paperless DREs represent a system problem that cannot be resolved by procedures. Established organizations such as the Brennan Center have concluded that paperless DREs are *not* trustworthy⁸, and the addition of VVPAT, audited to check machine tallies for accuracy, is the only way to *make* such systems trustworthy⁹. One must change the system itself: deploy an independent paper record of voter intent, confirmed by the voter, to use as the audit document and the true record of the vote.

Another critical function of voter-verified paper records, apart from security: VVPRs resolve the problems that occur when machine malfunctions result in lost electronic vote information.

A voter-verified paper record printer, for example, would have resolved the problem in Carteret County, NC in 2004 when 4500+ votes were irretrievably lost, affecting the outcome of a statewide race in which the margin was less than 2000.¹⁰ After that unfortunate (costly) event, NC passed a voter-verified paper record law. Each election, new examples arise – either of situations where votes were irretrievably lost, but could have been recovered if a VVPR requirement were in place, or of problems discovered and resolved because VVPR systems were in place.

MEANINGFUL AUDITS WITHOUT VOTER-VERIFICATION?

When Commissioner DeGregorio speaks of a HAVA “audit requirement”, he’s likely referencing Section 301(a)(2)(B)(i), indicating a permanent paper audit record must be produced. However, HAVA contains no corresponding language that says (a) the paper record must be voter-verified, nor (b) that the paper record must be used to cross check machine tallies for accuracy. Thirteen states have already explicitly required audits of the voter-verified paper records.¹¹

The suggestion that a reprint of unverifiable electronic ballot images, never reviewed nor confirmed accurate by the voters, can be used to conduct a meaningful audit has been soundly and repeatedly discredited. Just this month, the US League of Women Voters passed a resolution in support of the use of voter-verifiable paper ballots/records for routine audits, and decrying the lack of a recountable audit trail in “paperless” electronic voting systems.¹²

Although the EAC has not yet taken a position on VVPR, they may find it necessary to more directly address this groundswell of support in the near future, and it is hoped that they will soon discard the discredited assertion that non-voter-verifiable records are acceptable for audits.

HUMAN FACTORS

Committee concerns about human factors are well-placed. DREs have fallen short in several human factors areas, but the Commission's response only targeted one issue: VVPAT printer design. One usability success story is Michigan's VVPR system. When Michigan adopted precinct-based optical scan voting systems statewide, key reasons cited were simplicity of operation and design, the ability

⁸ U.S. GAO (see: <http://www.verifiedvoting.org/article.php?id=5826>), Johns Hopkins Institute, Raba Trusted Agent Report for MD's legislature and the Brennan Center's Task Force on Voting System Security: <http://www.brennancenter.org/programs/downloads/Full%20Report.pdf>

⁹ Carter-Baker Commission (see <http://www.verifiedvoting.org/article.php?id=5824>), CA Voting Systems Technology Advisory Board, League of Women Voters (June 2006)

¹⁰ <http://www.wral.com/news/3891488/detail.html>

¹¹ <http://verifiedvoting.org/downloads/ManualAudits-06-06.pdf>

¹² <http://www.verifiedvotingfoundation.org/article.php?id=6363>

to hand count ballots if necessary, and actual ballots to serve as an audit trail to resolve disputes over accuracy.¹³

DREs have fallen short in other areas on human factors and usability, especially with regard to meeting the needs of voters with disabilities. Given that one of the primary objectives of HAVA was to address disability access, it is most unfortunate the extent to which many of the newly purchased DRE systems have yet to adequately meet accessibility concerns, e.g.:

1. lack of interfaces for those with manual dexterity disabilities (with few exceptions)
2. need to insert smart-card, hard to manipulate by voters with manual dexterity disabilities
3. audio ballot interfaces cumbersome to the point of being unusable (one DRE's audio interface instructed blind voters to "push the yellow button").

Some voters with disabilities have documented these flaws.¹⁴ Many voting systems deemed "accessible" by the states buying them, fail utterly to meet the needs of voters with manual dexterity and mobility disabilities. Since most jurisdictions deploying such marginally-accessible equipment won't likely obtain new systems soon, it may be *years* before HAVA's intent is met.

Other problems include non-intuitive design issues that impact ALL voters: having to deselect a choice for Candidate A before being allowed to change one's selection to Candidate B, incorrect selections resulting from mis-calibrated touch screens, hypersensitive screens that erroneously register selections when none was intended, positioning of the summary-screen's "cast ballot" button in the same location on the touch-screen as the "next page" button, and more.

Compare the development of VVPAT printers to the evolution of seat belts in cars. Automobile vendors initially fought the requirement: "they won't be effective, they will cost too much, most people won't use them," etc. The first generation of seat belts were not so effective, not comfortable to wear, and most people didn't use them. However, the public and the government rejected arguments that requirements for seat belts were a bad idea, or that the push for seat belts should be abandoned because of poor initial implementation. Requirements expanded, and vendors produced more effective and more comfortable seat belts. Information campaigns target those who forget to buckle up.

VVPAT/VVPR requirements are the seat belts for our voting systems, a necessary protection to ensure those systems are secure, accurate, reliable, and auditable. Some vendors have been resistant to put significant effort into this technology, and some first generation VVPAT systems may not be well-designed, reliable, or user friendly. It is no surprise that some election officials may find such systems difficult to deploy or that some voters may not verify the printouts from VVPAT printers.¹⁵ Improved standards and public pressure will compel vendors to do a better job of implementation.

SECURITY VULNERABILITIES and CERTIFICATION

The Committee's question to the Commissioners about recently uncovered vulnerabilities was not fully answered. It is important to be absolutely clear: the defective Diebold systems made it all the way through the existing federal certification process, despite the fact that these security vulnerabilities that were first mentioned in January 2004,¹⁶ and recently expanded upon.¹⁷ No certification system, even improved over today's systems, can catch all such vulnerabilities.

¹³ http://www.michigan.gov/documents/Uniform_Voting_System_2_71047_7.pdf 2003

¹⁴ Silicon Valley Council of the Blind, <http://www.verifiedvoting.org/article.php?id=2117> ; reports by Noel Runyan and Kelley Pierce, <http://www.votersunite.org/info/accessibility.asp> and NAPAS, <http://verifiedvotingfoundation.org/napas>

¹⁵ Testimony to the EAC from a Nevada election official regarding their initial implementation of VVPAT printers somewhat contradicts these concerns for one vendor's design; he said it was relatively simple, in the particular system they used, to change the printer cartridges and it could be done during the voting day with minimal interruption.

¹⁶ http://www.raba.com/press/TA_Report_AccuVote.pdf

¹⁷ http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf (California Secretary of State); and www.blackboxvoting.org

Nor will a certification system catch ballot programming errors, since such programming is unique for each election and thus does not go through the certification process. Ballot programming errors (not uncommon, and generally representing honest mistakes rather than sinister plots) pose a very significant risk to the accuracy and verifiability of elections conducted on paperless DREs. Tighter certification systems will do nothing to protect against such risks.

While the expert who identified the specific vulnerabilities in the Diebold system/s was given access to those systems to examine them (and justifiably so, given earlier revelations about poor security design in these systems), we have no way of knowing if or how many other persons with sufficient access (and ill intent) may have quietly uncovered these vulnerabilities earlier.

Further, in some election jurisdictions, complete voting systems are sent home with pollworkers and kept at their homes (in some cases, even in their cars) for up to several weeks prior to election day. In other jurisdictions, voting systems may be delivered to polling places early and left insufficiently secured. Access is always a hazard; procedural safeguards alone cannot protect against these vulnerabilities. Only a system of VVPAT/VVPR coupled with mandatory manual audits of the VVPRs will detect (and permit recovery from) such errors.¹⁸

COMPUTERS EASY TO HACK

We agree fully that voting systems (which are indeed computers, despite what some officials claim to the contrary) are remarkably easy to hack. We would add that malfunctions which result in the loss of vote data are remarkably common.

Even assuming the best possible practices, such as thorough background checks of the ownership, management, and employees of vendors, meticulous and intrusive reviews of the design and manufacture of the equipment by truly independent experts – these measures would not eliminate programming errors and security holes. Despite any best-case scenario, there will always be people who can “hack” the machines (including the programmers who write the code in the first place).

Given the current state of technology, elections cannot be trustworthy unless there are voter-verified paper records of the votes and a significant portion of those paper records are manually counted to check the machine tallies.

RANDOM CHECKS

To carry out meaningful “random checks”, you need VVPRs to have something meaningful to check. The most effective way to provide a meaningful check on the proper functioning of voting systems for actual elections is by requiring mandatory manual audits of the VVPR from randomly-selected jurisdictions, as required by federal bills such as H.R. 550.

Parallel monitoring, sometimes proposed as an alternative way to “audit” the accuracy of voting systems during actual elections, cannot help where malfunctions result in lost vote data, and cannot resolve a discrepancy the monitoring might uncover. Paper records of voter intent can do both. (Parallel monitoring can also be tricked by malicious software.)

The testimony gives rise to a question: How does the Commission envision the EAC taking on random checks of voting systems around the country (absent the passage of legislation such as H.R. 550, which would fund such mandatory random manual audits nationwide)?

Verified Voting urges the Committee on House Administration to hold hearings on voter-verified paper record legislation as soon as possible. Passage of such legislation is most assuredly the fastest way to safeguard elections in those remaining states that do not yet require VVPR or audits.

¹⁸ <http://www.verifiedvotingfoundation.org/article.php?id=6355>