PRELIMINARY ANALYSIS OF E-VOTING PROBLEMS HIGHLIGHTS NEED FOR HEIGHTENED STANDARDS AND TESTING

NRC WHITEPAPER
DEIRDRE MULLIGAN,[1] JOSEPH LORENZO HALL[2]

Introduction

The computer science and voter protection communities were anxious leading up to the general election on November 2, 2004. Electronic voting machines, especially the increasingly popular paperless Direct Recording Electronic (DRE) voting machines, had received much scrutiny and it had become clear that DREs had numerous failings including a lack of end-to-end auditability and security and privacy vulnerabilities.[3,4] While the 2004 general election was not the technological nightmare some envisioned, there were isolated disasters, widespread reports of problems related to human factors and a number of tabulation irregularities, some of them recoverable, some not.

In a preliminary analysis, this whitepaper explores the relationship between current standards and certification procedures for voting systems and reports of technology failure during the 2004 general election. First, the paper briefly sets out the current standards and documents the gaps therein. Second, the paper sets out the certification process for voting systems. Third, the paper classifies and discusses representative examples of technology failure that occurred during the 2004 election. Finally, the paper examines the incidents of technology failure to identify why they were not caught through the various testing and certification procedures. The paper concludes that current voting system standards are inadequate; fully certified systems exhibited critical problems due to gaps in the standards and the certification process. For example, there are no federal guidelines that speak to human factor issues in electronic voting and many

complaints recorded by voter protection groups in the 2004 election specifically implicated issues of usability. In addition, the federal qualification system for DRE voting machines is inadequate and incomplete: it is evident that significant problems slipped through the cracks resulting in polling place or tabulation failures in 2004. The paper makes several recommendations to address the failures in standards and testing to ensure that problems with DRE voting systems evident in 2004 are corrected. In the specific case of counting failures, we conclude that the failures in 2004 provide ample evidence of the need for routine, end-to-end auditability using audit trails that represent the intent of the voter in DRE systems. The paper recommends that voting research, lying somewhere between basic and applied research, should receive additional funding.

Standards for Electronic Voting Equipment

Due to technical problems with voting equipment in the 1960s and early 1970s, the Federal Election Commission's (FEC) Office of Election Administration (OEA) requested that the National Bureau of Standards (NBS) (predecessor to the National Institute of Standards and Technology (NIST)) conduct two studies over the following decade. The first explored the use of computerized technology in vote tallying and found a need for guidelines for computerized vote-tallying systems.[5] This report argued that such standards would help election officials to normalize the difficulties inherent in making purchasing decisions in an environment with little computer expertise, little market leverage per election official and a staggering variety of state regulation that ranged from full independent testing to none whatsoever.[6] The second study explored the feasibility of developing voluntary standards for all voting systems.[7]

The end result was the FEC's Voting System Standards (VSS) published in 1990.[8] While establishing a set of voting equipment guidelines, the FEC 1990 VSS lacked guidance in the areas of security and privacy protection, human factors, voting system documentation, configuration management and quality assurance.[9] Those standards were not addressed and presumably deferred for a future VSS.

The VSS stagnated until 2002; voting systems vendors and election officials were left without guidance in the interim despite the fact that computerized voting technology continued to increase in sophistication.[10,11] Further, once new standards were put in place in 2002, a complex transitional plan resulted in vendors being allowed to submit their systems for a final qualification under the 1990 standards as long as they responded to any deficiencies within 60 days and the subsystems already qualified under 1990 were grandfathered in and thus exempt from the new standards.[12] This resulted in most vendors qualifying their systems under the old standards. Today, there are only two newer and rarely used systems qualified in whole or in part against the more recent voting system standards.[13] The majority of voting systems used during the 2004 election were qualified under the 1990 standards that were widely acknowledged to be outdated and incomplete in 1997.[14]

Changes in the 2002 guidelines included standards for security and privacy protection, accessibility, documentation and configuration. Currently, the 2002 VSS is the standard for federal qualification; the FEC's successor, the Election Assistance Commission, is beginning the process of updating the VSS. The 2002 VSS recognizes certain areas where standards were needed but not addressed: election administration functions, voter registration database integration, the use of commercial off-the-shelf (COTS) products,

remote networked (internet) voting,[15] and error measurement.[16] Notably, the VSS lacks standards or guidelines that speak effectively to issues of usability and auditability.[17,18] Despite the progress made in the 2002 VSS, substantial gaps remain.

Serious problems with balloting during the 2000 presidential election including incompletely punched punchcards and poorly performing lever machines contributed to 4 to 6 million lost votes according to one estimate.[19] These problems were answered legislatively with the Help America Vote Act of 2002. HAVA established the Election Assistance Commission, a clearinghouse for information and procedures involved in the administration of Federal Elections, provided mandatory minimum standards for voting systems, updated the voting system qualification process and provided funds to upgrade aging voting equipment. Unfortunately, the EAC commissioners were not appointed until late 2003 and funding for their work, including updating the VSS, was not fully appropriated.

The discussion above establishes the background of voting system standards for the technology used in the 2004 election. The 1990 standards were outdated by 1997, and new standards were not in place until 2002. Unfortunately, the vast majority of voting systems used in the 2004 election are qualified against the 1990 standards. As well, voting systems that meet the 2002 standards may not meet the minimum requirements under HAVA and certainly do not incorporate requirements such as usability where the need has been documented but to date no standards have been promulgated. In the

remainder of this paper, we highlight the need for usability and auditability standards and testing as seen through the problems with the 2004 elections.[*]

Testing Electronic Voting Equipment

On Election Day, the intent of voters merges with the voting technology they use. With paperless systems such as DRE voting machines and lever machines that provide no Voter-Verified Audit Trail[20] (VVAT), any failure that affects the recording of the vote or the integrity of vote data can cause unrecoverable errors. In contrast, with paper-based systems, individual records can be recounted as a check against tabulation software.

To ensure they function and properly record voters' intent, voting technologies are subject to a variety of tests by external entities. In addition to the vendor's internal quality assurance procedures and testing, conformance testing against federal voting systems standards, certification testing against state regulations and procedures, and local acceptance testing of voting equipment is required in most jurisdictions to ensure that each voting system delivered operates as expected.[21] As we discuss, the lack of core standards in certain areas and ineffective testing undermine the goal of assuring the integrity and reliability of voting systems.

Vendor Quality Assurance Testing

Voting system vendors test their voting systems. The goal of such Quality Assurance testing (QA) is to ensure that a voting system will perform as intended outside of the lab. This testing can be simple or elaborate and increased QA costs are undoubtedly passed on to the county or municipality. The voting technology market is small and highly competitive; there is an opportunity cost between low-cost and well-designed products.[22]

---

[*] We will incorporate other needs, such as privacy and accountability, in the future. See note 18.

Due to the level of secrecy and proprietary protection in the voting technology market, a reasonably complete survey of vendor QA processes is not available.[23] In such a highly competitive environment that is mission critical to the functioning of a representative democracy, and in which outcomes are decided by razor-thin margins, vendor QA cannot on its own be relied upon to provide proof of performance. The importance of external review is heightened by recent findings that one vendor, Diebold, sold faulty products and made misrepresentations in California[24,25] and posed "considerable security risks" for Maryland's election system.[26]

Federal Qualification Testing

As outlined above, the FEC established a set of voluntary Voting System Standards (VSS) in 1990 that were updated in 2002. The 2002 standards include:

- **Performance Standards** for functional capabilities, hardware, software, telecommunications, security, quality assurance (QA), and configuration management (CM).
- **Testing Standards** for the technical data package, functionality testing, hardware testing, software testing, system integration testing and CM & QA testing.

Voting systems are tested against the VSS by Independent Testing Authorities (ITAs) that are certified to conduct these tests by the National Association of State Election Directors (NASED).[27]. ITAs certified to test voting systems are Wyle Laboratories (hardware) and CIBER, Inc. (software) of Huntsville, Alabama and SysTest Laboratories (both hardware and software) of Denver, Colorado. These ITAs conduct manual and automated source code review, documentation review, environmental "shake-and-bake" testing, and some systems-level testing of the full voting system.[28] Due to the voluntary

nature of federal qualification, the vendor pays for ITA testing and all reports are proprietary. Besides the eventual transmission of the qualification report from the ITAs to NASED/EAC which is the basis for being "NASED qualified," the process is completely closed to the public and other third parties; there is no indication as to what specific tests are conducted to verify that a system fulfills the VSS and no publication of problems encountered during testing. What little insight that exists into ITA testing comes from sparse public comment and state access to ITA reports during state certification.[29,30] Each voting system, that does not predate the VSS themselves,[31] must pass both hardware and software testing by an ITA before it is considered "federally qualified" and given a NASED identification number.[32] However, voting subsystems – for example, polling place DREs or central election management systems – do not have to be requalified if already submitted; the end result is that the vast majority of voting systems are currently certified against the 1990 standards, and there are no signs that vendors will cease their aggressive marketing of these older systems.[33]

State Certification Testing

States may or may not require voting machines they purchase and use to have federal qualification. Some states further regulate and test voting systems to ensure that they meet specific local requirements absent from the federal qualification process or they may require additional testing where the state has found federal qualification to be deficient. Specifically, 35 states require both federal qualification and additional state certification, 9 require only federal qualification, 5 require only state certification (Arizona, New Hampshire, New Jersey, North Carolina and Vermont) and 2 require neither federal qualification nor state certification (Mississippi and Oklahoma).[34]

A few states – Ohio, Maryland and California – have hired independent technical consultants to evaluate voting systems.[35] One report, using "red team" exercises in an election-day environment, by RABA Technologies Innovative Solution Cell found "considerable security risks" with Maryland's election system.[36] Around the same time as the RABA report, election officials in California became aware that one voting system vendor was misleading local election officials and violating California Election Code by installing software on voting systems that had not yet been approved by the state.[37] California Secretary of State Kevin Shelley acted quickly to put into place regulations that required voting systems to undergo an unprecedented level of certification on top of ITA certification. Secretary of State Shelley found it necessary to mandate an accessible voter-verified paper audit trail (VVPAT) and, for systems that are not designed to produce a VVPAT, vendors must agree to a full source code review by technicians of the Secretary of State's choosing, parallel monitoring, detailed security planning, and detailed computer security requirements.[38]

Local Acceptance Testing

Immediately before, during and after elections, the county or municipality must ensure that voting systems are used in a manner that maintains their physical security and system integrity and does not disenfranchise voters. The level of local regulation varies widely across the more than 10,000 election jurisdictions in the United States.[39] For example, some counties deliver voting equipment on the morning of Election Day while others deliver it weeks ahead without adequate protection for the equipment's physical security and integrity. The quality and degree of local election regulation and administration varies substantially and an adequate treatment is beyond the scope of this whitepaper.

Local elections officials are responsible for training elections workers, overseeing the process of tabulation and certifying election results.

A Preliminary Analysis of Reported Problems

The standards and conformance testing process can itself be measured through sampling problems voters experienced on Election Day and problems that surfaced afterwards. The presidential election of 2004 saw reports of serious problems despite increased scrutiny of all aspects of voting technology in the electoral process. *The analysis below is preliminary; many of the incidents we discuss are still under investigation by election officials and election protection organizations.*

Reports of Problems with the 2004 Election

There were many reported problems with voting systems during the 2004 election. The Election Protection Coalition (EPC) recorded over 23,000 incident reports on Election Day using the Election Incident Reporting System (EIRS) and EPC's 866-OUR-VOTE hotline.[40] As well, the House Judiciary Committee has reportedly received 57,000 complaints of election irregularities.[41] While the preliminary analysis below is based on EPC data and press reports, we intend to conduct a more comprehensive analysis that maps specific incidents to gaps in the standards and testing process that would include the House Judiciary Committee's data.

From the EIRS incident reports, approximately 2,000 of these were related to problems with voting technology, most were in the areas of human factors and machine failure. It is important to emphasize some limitations of data collected by the EIRS. The data doesn't include counting or tabulation errors; these typically come out in the press during the days following an election during the official canvass. Naturally, this means that the data

is heavily slanted towards human factors issues as voters (humans) are reporting problems they had with the machine or perceived irregularities with election administration. Further, EIRS reports are from *voters* on Election Day who are not voting system experts and may not know much about their voting system. All of the EIRS data should be considered preliminary as, at the time of writing, election protection organizations are currently following up on reports that obviously necessitate further investigation. Tabulation errors, problems with counting individual ballots accurately, typically arise after votes have been cast; therefore the problems are not visible to individual voters but generally are identified by election officials and observers during the counting process. The details of tabulation failures are frequently reported in the press. In this section, we discuss both problems reported by voters to the EPC election protection hotline and tabulation-related problems reported in the press in the weeks after November 2, 2004.

Human Factors Problems

There are currently no comprehensive federal standards and testing requirements for the usability of voting systems.[42] Usability problems are evident to the voter in the polling place and therefore comprise the majority of voter-reported problems logged by election protection volunteers.

In cooperation with the Election Protection Coalition[43] (EPC), VerifiedVoting.org[44] and Computer Professionals for Social Responsibility[45] collaborated to develop the Election Incident Reporting System[46] (EIRS) to record voter-reported problems on Election Day. EIRS is a suite of web-based software tools designed to record information about election incidents reported to a hotline (866-OUR-VOTE). EIRS facilitates real-time response to

election incidents by election protection attorneys and non-partisan election observers. On November 2, 2004, over 2014 individual election incidents were recorded that EPC volunteers classified as "machine-related" election incidents. We provide summary statistical data in Tables 1 and 2 attached to this paper. Notably, over 75% of all machine-related election incidents were reported from counties that use paperless voting technology and 5 vendors were responsible for approximately 90% of all incident reports. The vast majority of these incidents were simple statements such as, "The machines are down" or "machines broken in my precinct" however approximately 218 of these incidents (10%) contained specific information that merits further analysis.

Reports of Human Factors Problems[47]

Machines Failing to Operate Normally

Machines crashed during voting, were rebooted, reset and/or repaired. In Palm Beach Co., FL a machine crashed and was rebooted.[48] In Philadelphia Co., PN, Kings Co., NY machines were repaired during Election Day and the nature of the repairs was unknown.[49] There were reports of EVM crashes or errors displayed while the voter voted[50] or crashing repeatedly during Election Day.[51]

Voters Experiencing Considerable Difficulty Casting Ballots

When voters reviewed their ballot before casting, some votes were misrecorded. EIRS recorded many reports (over 50) across all states and most types of electronic voting machine (EVM) of votes being misrecorded. These errors were only caught when reviewing the summary or review screen.[52] In a few cases, it took the voter five, seven and even nine attempts of going back and correcting their ballot choices for the proper vote to register.[53] This was reported primarily with presidential votes "jumping" from

Sen. John Kerry to President George W. Bush, but also vice-versa,[54] from Sen. John Kerry to third-party candidates[55] and for non-presidential races.[56]

Selecting one choice resulted in a different choice being selected or no choice selected. In Mercer Co. and Philadelphia Co., PN voters found it difficult to select choices on the Unilect Patriot and ELECTronic 1242 voting systems.[57] In Philadelphia and Albuquerque, some voters that pressed the button for straight-party Democratic ticket ballot instead had the lights for Republicans candidates light up.[58] Reports from New Mexico,[59] Kentucky,[60] Pennsylvania[61] and Ohio[62] said that certain machines ballots were skewed or certain choices refused to light up likely due to burnt out lights on a button-matrix machine.[63] In a number of cases, voters reported that DRE voting machines already had votes selected when they entered the voting booth.[64]

On some machines, it is easy for the voter to mistakenly cast a vote before they are finished voting or neglect to cast it at all. In Philadelphia Co., PN, Albuquerque, NM and Franklin Co., OH voters using the ELECTronic 1242 voting machines often mistakenly hit the "Vote" button after selecting choices in each race – which resulted in only their initial choice being cast – instead of waiting until they had finished making all their choices.[65] Voters reported accidentally brushing up against the touchscreen and accidentally casting their vote on Sequoia AVC Edge and Hart Intercivic eSlate machines.[66] Voters in Texas, Louisiana, Alabama, New Jersey, Pennsylvania and South Carolina using button-matrix DRE voting machines complained that they entered the booth and the previous voter's ballot had not been cast.[67]

In a few cases, disabled accommodations did not function properly or problems with multilingual ballot support rendered voting difficult or impossible. In Miami-Dade Co.

and Hillsborough Co., FL a voter reported that the audio voting interface only allowed voting for George W. Bush.[68] There were also situations where voting would be delayed for a considerable amount of time as poll workers had to bring an EVM out to a disabled person[69] who could not enter the polling place.[70] In Palm Beach and Broward Counties, Florida, there were reports of machines not allowing voting in English or only allowing part of the ballot to be displayed in English.[71]

Discussion of Reports of Human Factors Problems

Many of the human factors problems listed above could be addressed with high-level usability standards and user testing and evaluation.

Problems with Normal Operation of Voting Machines

Voting systems should be stable on Election Day. Crashes should not happen to a well-designed system in the first place, but if they do, they should be such that the voter consistently knows if their vote was counted.[72] Did these machines crash during the testing process? If not, what is different about the operating environment of the precincts in which crashes were reported compared to the testing environment? Answers to questions like this should be used as feedback into the testing process to reduce the likelihood that voting systems crash during voting. A testing process that attempts to mimic the use of voting systems as used in actual voting environments should be able to reproduce system crashes, catching them before Election Day. There is little publicly available documentation covering what happens during the boot-up of voting machines and some machines may even write votes to memory as they perform routine logic and accuracy tests during start-up.[73]

Problems with Casting Ballots

Vendors and election officials attributed "vote jumping" problems to touchscreen recalibration,[74] however, calibration is not specific to certain pages of a ballot but should be systematic; all or most pages of the ballot should show incorrect choices. Reports that correcting these mistakes took multiple tries are troubling; it should not be burdensome to change an incorrect choice so that the voter's electronic ballot reflects their preferences. This type of usability test case – where systems are tested to evaluate how easy a vote can be miscast and then corrected – are absent from the federal qualification process. It would seem that such behavior would be readily apparent during user testing contemplated as part of a future EAC human factor standard.[75]

In cases where it is too difficult or too easy for voters to make a selection in touchscreen systems, there is a need for standards that specify what degree of force should be considered to be a "choice" and, in general, what parameters define a successful voting process. Having voting systems designed to proper tolerances would, for example, reduce the amount of inadvertent choices made. Button-matrix machines have many moving parts and certain buttons are inevitably pressed with a higher frequency on Election Day.[76] It is essential that moving parts on the balloting interface – buttons, levers, lightbulbs that indicate choices – are tested on each machine during logic and accuracy testing prior to each election and that such parts can be replaced on machines quickly during an election without compromising the integrity of the machine.

It is also troubling that systems are designed such that voters inadvertently cast their vote or leave the voting booth without casting a vote. While making choices in individual races should be easy, certain processes – such as casting a ballot – should not be as trivial. This could be addressed by a standard that said "Voting systems shall minimize

the likelihood of inadvertently casting a ballot or leaving the voting booth without having cast a ballot." For example, a simple feedback interface on touchscreen DREs that asks, "Are you sure you are done voting and would like to cast your ballot?" or a mechanical construct on button-matrix DREs that requires the voter to first attest that they are done voting and *then* that they are ready to cast their ballot, in two steps, could reduce the likelihood of premature and incomplete voting. Also, in voting systems that don't require a authorized token (such as a smartcard) to be removed from the machine before the voter is done voting, this behavior can be mimicked with other types of tokens. Usability testing using a reasonable distribution of actual voters would likely reveal problems that resulted in premature or incomplete voting.

Finally, testing of the audio voting interface is just as important to the functioning of an accessible EVM as the primary interface.[77] Any specific incompleteness or deficiency in the audio ballot should be recognized and remedied during local acceptance testing or logic and accuracy testing while higher-level usability problems with accessible interfaces should be caught in federal qualification testing. Vendors should take the advice of usability experts to incorporate User-Centered Design (UCD) processes that use a distribution of real users – disabled and non – in actual tests during design, development and debugging of their systems.[78]

Tabulation Problems

Tabulation problems – where votes are not counted as intended to be cast by voters – come in two varieties, recoverable and unrecoverable. Recoverable tabulation problems are such that a redundant or official record of voter intent can be recounted if a primary record, such as an aggregate tally, is clearly erroneous. Unrecoverable problems do not

permit recounting of voter intent, and, in particularly egregious cases, require an election to be redone. In the lists below, we have included representative examples of tabulation errors separated into two categories – those on paperless and paper-based systems – to highlight that the paper-based tabulation errors are more often than not, recoverable.[79]

Paperless Systems

Voting systems that do not keep independent, indelible records of the voter's intent are the most likely to suffer from unrecoverable errors resulting in lost votes or low-confidence aggregate tally numbers. While HAVA does require that voting systems provide certain features with respect to auditability,[80] it is clear that comprehensive standards for voting system auditability are needed as paperless and paper-based voting systems enjoy different degrees of auditability and recountability.[81] In the weeks following the November 2004 election, a number of tabulation problems surfaced in the media that illustrated this disparity.

Reports of Tabulation Problems with Paperless Systems

Cateret Co., NC – Too many early voters voted on Cateret County's Unilect Patriot voting system. The system could store only approximately 3,500 ballots; over 8,000 voters voted early resulting in the complete loss of more than 4,500 votes.[82] The election will likely have to be redone for at least one race at a cost of $3 million.[83]

Columbus, OH – An error while a Danaher / Guardian ELECTronic 1242 was plugged into a laptop to download results gave President Bush 3,893 extra votes.[84]

Gastonia, NC – Equipment failed to count 12,000 early votes due to an "interrupted download" error.[85] Over half of Gaston's polling places recorded too few or too many

votes when compared to the number of registered voters who signed the registration poll books.[86]

Mecklenburg Co., NC – 106,064 early and absentee votes are counted where only 102,109 actually voted. The cause of the error is still unknown.[87]

Discussion of Reports of Tabulation Problems with Paperless Systems

The Cateret County case was relatively straightforward. When the Unliect Patriot voting system's memory is full, it displays an error message, "Voter Log Full," only until the system is reset to allow the next voter to vote. Further, the ballot counter, that displays how many ballots have been cast since the opening of the polls, continued to advance despite the ballots it was counting not being recorded in memory. This points to a gap in the voting systems standards: voting systems should not allow ballots to be cast on them if their memory is full. Testing should be modified to test for these types of conditions. Finally, if there existed more robust auditability standards that specified a voter-verified audit trail independent of the voting system software, these records could be recounted to recover the 4,500 lost votes and the election would not have to be held again.

Although not a lot is known about the errors, discussed above, in Columbus, Ohio and Gaston, NC, it appears that a transmission error during downloading data from a voting machine caused erroneous data to be inserted into or excluded from the vote tally, respectively. In computer networking, there are commonly used methods to ensure that the receiving end of a communication can check to make sure that the message has arrived uncorrupted. Although networked voting systems have larger security implications beyond the scope of this whitepaper, it would seem reasonable to require that networked voting systems incorporate transmission error correction to avoid

inadvertent or malicious corruption of vote tallies. The 2002 VSS do specify a data integrity requirement that would have alleviated this.[88] However, as is the case with most qualified election systems on the market, the ELECTronic 1242 – used in Columbus – and the Diebold AccuVote-TS – used in Gaston – are qualified against the 1990 VSS;[89] voting system standards relevant for computerized voting technology from 15 years ago.

One of the few ways to know beyond a shadow of a doubt that a county has a problem with its DRE equipment is if drastically fewer or greater votes are recorded by the system when compared to the number of voters that sign registration poll books. Unfortunately, without a robust end-to-end audit capability, such errors can be very mysterious. The end result is that the entire election may be called into question while in paper-based systems a manual recount can be conducted.

Paper-based Systems

Reports of Tabulation Problems with Paper-based Systems

Broward and Orange Cos., FL – Software provided by Election Systems and Software (ES&S) on the optical scan machines used for counting absentee votes only read 32,000 votes and then started to count backwards.[90]

Volusia Co., FL – Seven Diebold optical-scan machines had memory card failures causing, for example, 13,244 votes to disappear from one card's tally.[91]

LaPorte County, IN – A bug in ES&S' punchcard tabulation software causes each precinct to be reported as only having (exactly) 300 voters each; all reports add up to 22,000 voters in a county that has more than 79,000 registered voters.[92]

San Francisco, CA – A glitch in the new tabulation software made by ES&S to handle Ranked-Choice Voting for optical scan machines stopped the counting and forced a recount of 81,000 ballots.[93]

10 Counties in North Carolina – A database error with Fidlar & Chambers optical-scan equipment counted straight-party Democratic votes as straight-party Libertarian ballots; a recount changed the outcome in one race.[94]

Utah County, UT - 33,000 straight-party ballots are not counted due to a programming error in punchcard counting equipment.[95]

Discussion of Reports of Problems with Paper-based Systems

This is a remarkable list if for only its diversity of voting technology – from punchcard to optically scanned paper ballots – and heavy preponderance of software errors. In fact, further details surrounding the problems above are not necessary. That is, while it would be better if these errors were caught in the testing process, the existence of a voter-verified audit trail – the paper ballots – ensured that the election could be tallied independent of the problems with the tabulation equipment and software. In a future analysis we aim to further scrutinize problem reports with paper-based voting systems that used computerized technology to highlight that they are also not being adequately tested. However, for now, we merely point out that errors on paper-based systems are recoverable.

Findings

From a quick analysis of EIRS data (see Tables 1 and 2 attached) and press reports, we report the following findings:

- Approximately 30% of voter-reported incidents were from counties that use two older, button-matrix DRE voting machines – The ELECTronic 1242 by Guardian Voting Systems and the Sequoia AVC Advantage.

These two machines were designed and implemented using technology over 15 years old; in terms of computing advancement, they are Babylonian. Both are qualified against the 1990 standards and, as such, only require changes in their software to be re-certified in the future.[96] There is no prohibition on selling outdated voting technology qualified against obsolete standards, and the vendors show no sign of ceasing their aggressive marketing of these two machines.

- Approximately 75% of all EIRS election incidents concerned DRE voting machines and lever machines.

From the EIRS data, DRE machines and lever machines seem to be the most problematic in terms of human factors. Increasing use of DRE machines will likely result in these problems becoming more widespread.

- 70% of all EIRS incidents were from six voting systems.
- 90% of all EIRS incident reports are associated with five vendors – ES&S, Sequoia, Danaher, Diebold and AVM – out of approximately thirty-one.[97]

If these findings are representative, and not an artifact of the EIRS sample, this means that a small amount of voting system vendors are responsible for the lion's share of human factor-related polling place problems. Without further knowledge of vendor quality assurance (QA) procedures it is not possible explore the correlation of vendor QA with the amount of problems reported by voters.

- Many tabulation errors implicated technical problems that are addressed in the 2002 VSS. However, only two newer and rarely used voting systems are qualified in whole or part against the 2002 standards.[98]

The twelve-year lag in updating the voting system standards has left us with voting technology that is overwhelmingly qualified against outdated standards. This leaves the nation in a state where the current standards are effectively irrelevant to voting technology actually supplied by the market. When the VSS is finally updated again, will we still have obsolete, ineffective voting technology certified, marketed and sold more than two years after they come into effect?

- Certain tabulation errors implicated problems where there exist no voting system standards – especially in the area of auditability – or where testing is not sufficient.

Problems discussed in the analysis above where thousands of votes were "lost" from or "inserted" into a tally and problems that implicate common computer programming mistakes simultaneously point to the need for higher-quality performance-based testing to catch these errors before Election Day and end-to-end auditability to detect and recover from those that slip through the cracks.

Recommendations

- High-level, comprehensive usability standards should be a part of the next voting systems standard to ensure reliable casting of votes.

- Usability testing involving expert review, scripted observation and field tests using a realistic distribution of actual users should be part of federal qualification.[99]

Problems related to human factors have been endemic in electronic voting. They will continue to be problematic until voting systems are required to meet a reasonable level of usability. The federal qualification process should test voting systems against such standards using usability expert review incorporating the latest knowledge, actual voters in simulated and real election situations. Catching problems before Election Day is essential to ensure that all voters can reliably cast votes.

- Standards for end-to-end auditability should be in place to ensure the integrity of elections conducted on DREs.
- Testing routine end-to-end audits to demonstrate that a voting system is fully recountable should be part of federal qualification.

While HAVA fleetingly addresses auditability in its mandatory minimum requirements, they do not approach the level necessary for end-to-end auditability. An indelible, independent manifestation of voter intent is necessary to ensure that jurisdictions can recount their votes when needed or as provided by law. As well, there must be a process or mechanism in place to ensure that instruments of auditability are used effectively. Auditability testing should also be part of the federal qualification process and jurisdictions should be required by states to conduct routine audits – as opposed to the simple, predictable case of a recount[100] – to detect malfunction and malfeasance.

- The testing of voting systems needs an overhaul to move from functional testing to performance-based testing.
- There should be a rich feedback loop – from problems to investigation to testing – that uses actual problems to inform testing procedures.

It is evident from the problems surrounding the 2004 election that many bugs, glitches and poorly designed features make it through the complicated net of voting standards and testing. A large improvement could be had by moving from the current regime of functional testing – where a system is literally checked off for compliance with the 1990 or 2002 VSS – to performance-based testing – where systems must perform in a specified manner and tests attempt to adversarially compromise this performance. Ultimately, testing ignorant of problems experienced in the field is shortsighted; there should exist a rich feedback loop into federal qualification testing. Investigations of problem reports can be used to test if problems experienced in the field have been addressed by vendors and can be used to redesign the testing environment so that fewer problems make it through the process.

- Voting research can help to identify current and potential problems with election systems as well as inform new innovative designs.

There is a general lack of high-quality information and research in the areas of usability, security and privacy of voting systems. There is also a need for research into and aggregation of information about voting technology, election administration and accountability, best practices and election law. The next generation of voting research might involve qualitative assessment of voter behavior and knowledge as well as research into alternative election systems altogether. Attracting talent to these research areas is

essential to stimulate innovation in voting systems and for a better understanding of the complexities of such a critical system.

Conclusion

In terms of voting technology, the 2004 Election was uneventful in some areas and a total disaster in others. Problems with election technology undoubtedly caused lost votes, miscast votes and significant disenfranchisement of voters. The FEC's 1990 and 2002 Voting System Standards serve a valuable function but are still considerably lacking in the areas of human factors and auditability.

Human factors issues are a majority of the problems voters experience with voting technology on Election Day. Federal standards could alleviate routine design errors. More research into the usability of electronic voting machines is necessary to understand how certain errors happen, the spectrum of user behavior, and how to design hardware and software that reduce confusion and human error.

Unfortunately, the lack of end-to-end auditability in modern DREs means that only cursory audit capability is available – such as making sure that the number of votes cast is equal to the number of signatures in the poll books. Without a fixed record on which voters verify their intent, recounts are meaningless and, sophisticated fraud such as vote switching is undetectable. Auditability standards specifying a VVAT and routinely conducted random audits would go a long way towards detecting fraud and malfunction and ensuring that there is a back-up for recounting if needed.

As mentioned above, there is a need for usability research in electronic voting. However, further statistical research into machine failure rates, polling place errors and

investigation of election incidents as well as novel qualitative research would also help to build a more complete picture of our election system, its strengths and its weaknesses.

Voting System	Percent
Danaher/Guardian ELECTronic 1242	17.87
AVM Lever Machine	11.68
Sequoia AVC Advantage	10.70
ES&S iVotronic	10.65
Diebold (Optical Scan)	9.40
ES&S Punchcard	9.29
Sequoia AVC Edge	7.77
ES&S Optical Scan	6.25
Diebold AccuVote-TS	4.29
Hart eSlate	3.15
InkaVote	2.23
Unilect Patriot	2.12
Unkown optical scan (Diebold?)	0.98
Sequoia Optical Scan	0.92
ES&S Optical Scan / Sequoia AVC Edge	0.65
AVS (Shoup) Lever	0.43
AVS WinVote	0.38
MicroVote MV-464	0.38
ES&S EV-2000	0.27
Unknown punchcard	0.22
Unknown	0.16
ES&S Votronic	0.11
Mixed Optical Scan	0.11
Total	100.00

Table 1. This table shows the percentage of machine-related EIRS incident reports for each voting system. The list of machine-related incidents was groomed from 2014 initial incident reports to a list of 1985 that had identifiable counties. Then, 144 counties were rejected where only one incident was reported. Finally, using the Verified Voting Foundation's Verifier Database,[†] we associated each of the remaining counties with its voting system. The resulting sample contains 1841 election incidents from 138 counties – 90% of the raw data.

[†] See http://www.verifiedvoting.org/verifier/ .

Vendor	Percent
ES&S	27.21
Sequoia	19.39
Danaher	17.87
Diebold	13.69
AVM	11.68
Hart	3.15
InkaVote	2.23
Unilect	2.12
Unkown	1.47
AVS	0.81
MicroVote	0.38
Total	100.00

Table 2. This table is essentially the same as Table 1 but by vendor instead of a specific voting system.

[1] Director, Samuelson Law, Technology & Public Policy Clinic, Acting Clinical Professor, Boalt Hall, University of California, 346 North Addition, Berkeley, CA 94720-7200, (510) 643-4625, dmulligan@law.berkeley.edu, http://www.samuelsonclinic.org

[2] PhD Student at the School of Information Management and Systems (SIMS), University of California, 102 South Hall, Berkeley, CA 94720-4600, joehall@berkeley.edu, http://sims.berkeley.edu/~jhall/

[3] D.W. Jones, *Auditing Elections*, 47 Communications of the ACM 46, October 2004, available at http://doi.acm.org/10.1145/1022594.1022622 .

[4] For a representative discussion of problems with electronic voting machines see 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), available at http://avirubin.com/vote.pdf

[5] Roy Saltman, *Effective Use of Computing Technology in Vote Tallying*, Institute for Computer Science and Technology: National Bureau of Standards, NBSIR 75-687, (1975), available at http://www.vote.caltech.edu/Reports/NBS_SP_500-30.pdf .

[6] See of Eddan Katz and Rebecca Bolin, *Electronic Voting Machines and the Standards-Setting Process* (May 2004), at 2, (unpublished manuscript, on file with authors).

[7] National Clearinghouse of Election Administration, Federal Election Commission: *Voting System Standards: A Report on the Feasibility of Developing Voluntary Standards for Voting Equipment*, (1984).

[8] Federal Election Commission, *Performance and Test Standards for Punch card, Marksense and Direct Recording Electronic Voting Systems* (1990), available at http://sims.berkeley.edu/~jhall/fec_vss_1990_pdf/FEC_1990_Voting_System_Standards.pdf .

[9] United States General Accounting Office, *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (2001), at 8-10, available at http://www.gao.gov/cgi-bin/getrpt?gao-02-52

[10] Federal Election Commission, *Voting Systems Standards,* (2002), available at MS-DOC: http://www.fec.gov/pages/vssfinal/vss.html PDF: http://sims.berkeley.edu/~jhall/fec_vss_2002_pdf/ .

[11] *Supra., Elections: Status and Use of Federal Voting Equipment Standards*, at 11-12.

[12] Federal Election Commission, *A Plan for Implementing the 2002 Voting System Standards,* (2002), available at http://web.archive.org/web/20030112094804/http://www.fec.gov/pages/vssfinal/vss_implementation.html . (this document has been removed from the FEC website but is still available through the Internet Archive.)

[13] The Avante Vote-Trakker is fully qualified – that is, both the hardware and software for their precinct counter and central tabulation system – to the 2002 VSS. Diebold's AccuVote-TSx precinct counter is qualified against the 2002 VSS but the rest of its system is not. See National Association of State Election Directors, *List of Voting Systems that are NASED Qualified*, January 3, 2003, available at http://www.nased.org/NASEDApprovedSystems1.03.pdf .

[14] *Supra., Elections: Status and Use of Federal Voting Equipment Standards*, at 2.

[15] Computer security experts have recently discredited internet voting entirely. D.R. Jefferson, A.D. Rubin, B. Simons, and D. Wagner. *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*, www.servesecurityreport.org/ ; D.R. Jefferson, A.D. Rubin, B. Simons, and D. Wagner. *Analyzing Internet Voting Security; An extensive assessment of a proposed Internet-based voting system*, 47 Communications of the ACM 59, October 2004, available at http://doi.acm.org/10.1145/1022594.1022624 .

[16] *Supra., Voting Systems Standards, (2002), Overview,* at 6-7.

[17] *Supra., Elections: Status and Use of Federal Voting Equipment Standards*, at 11.

[18] The current discussion will focus on usability and auditability standards. However, we see evidence from the 2004 election for standards that contemplate issues of privacy and conflicts of interest: there were reports of voting systems and procedures not permitting sufficient privacy and vendor employees servicing machines and assisting in tabulation procedures. We do not discuss these issues here in the interest of time and space. All of these issues are arguably undervalued in the standards and testing process for voting systems.

[19] Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be* (July, 2001), at 8-10, available at http://www.vote.caltech.edu/Reports/

[20] A VVAT is a contemporaneously produced record of the voter's ballot that the voter inspects before casting their vote. A Voter-Verified Paper Audit Trail (VVPAT) is a VVAT that uses paper as the recording medium.

[21] *Supra., Electronic Voting Machines and the Standards-Setting Process*, at 9-11.

[22] Congressional Research Service Report RL30773, *Voting Technology in the United States: Overview and Issues for Congress* (2001), by Eric Fischer, at 18, available at http://usinfo.state.gov/usa/infousa/politics/voting/rl30773.pdf ; also see *Id., Voting: What Is, What Could Be*, at 53-54.

[23] It is notable that a whole section of the FEC's 2002 VSS is devoted to QA (*Id.*, *Voting System Standards (2002)*, Volume I, Section 7). However, the ITA reports that certify vendors' internal QA processes are protected proprietary information. Recent efforts to get ITA reports under Freedom of Information Act requests and their state equivalents may shed some light onto vendors' QA processes.

[24] Helen Gao, *Faulty Switches Cited in Voting Woes*, San Diego Union Tribune, April 14, 2004, available at http://www.signonsandiego.com/uniontrib/20040414/news_6m14diebold.html

[25] For example, Diebold was recently found to have knowingly sold unqualified voting hardware and software in the State of California. See Kim Zetter, *E-Voting Undermined by Sloppiness,* Wired News, December 17, 2003, available at http://www.wired.com/news/evote/0,2645,61637,00.html and; Kim Zetter, *Diebold May Face Criminal Charges*, Wired News, April 23, 2004, available at http://www.wired.com/news/evote/0,2645,63191,00.html .

[26] RABA Technology's Innovative Solution Cell, *Trusted Agent Report – Diebold AccuVote-TS Voting System*, January 20, 2004, at 3, available at http://www.raba.com/press/TA_Report_AccuVote.pdf

[27] National Association of State Election Directors, *General Overview for Getting a Voting System Qualified*, available at http://www.nased.org/NASEDITAProcess.pdf

Note: The Election Assistance Commission has taken over the roles of the FEC and NASED in the qualification process.

[28] C. Coggins, *Independent Testing of Voting Systems*, 47 Communications of the ACM 34, October 2004, available at http://doi.acm.org/10.1145/1022594.1022619 .

[29] *Id.*

[30] The authors have heard anecdotally that vendors are reluctant to give access to ITA reports even during the state certification process.

[31] Older, button-matrix DRE systems (see note 63 *infra*), such as the ELECTronic 1242 manufactured by Guardian Voting Systems, Inc. and the AVC Advantage manufactured by Sequoia Voting Systems, Inc. were "grandfathered" in to the federal qualification system so that counties that used these systems would not have to purchase entirely new voting systems. These systems are not subject to the same hardware tests as newer systems. These voting machines represent 1/3 of all DREs used in the nation or 10% of all precincts and vendors are still selling and aggressively marketing them. See p. 10 of Election Data Services, *Overview of Voting Equipment Usage in the United States, Direct Recording Electronic (DRE) Voting*, Statement of Kimball Brace to the EAC, May 5, 2004, available at http://www.electiondataservices.com/EDSInc_DREoverview.pdf

[32] *Supra., Independent Testing of Voting Systems.*

[33] *Supra., List of Voting Systems that are NASED Qualified.*

[34] *Supra., Electronic Voting Machines and the Standards-Setting Process,* at 11. (citing p. 3 of Election Reform Information Project, *Securing the Vote,* (April, 2004), available at http://electionline.org/site/docs/pdf/EB7_new.pdf)

[35] For example, see (OH) Compuware Corporation, *Direct Recording Electronic (DRE) Technical Security Assessment Report* (2003), available at http://www.sos.state.oh.us/sos/hava/files/compuware.pdf ; (MD) Science Applications International Corporation, *Risk Assessment Report: Diebold Accuvote-TS Voting System and Processes (redacted)*, SAIC-6099-2003-261 (2003), available at http://www.dbm.maryland.gov/SBE ; (CA) §§ 5(a)(3)(a)-(d) of: The Honorable Kevin Shelley, Secretary of State of the State of California, *Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems,* (March 18, 2004), available at http://www.ss.ca.gov/elections/ks_dre_papers/decert1.pdf (requiring vendors to provide code and documentation to a analyst of the California Secretary of State's choosing).

[36] *Supra., Trusted Agent Report – Diebold AccuVote-TS Voting System.*

[37] *Supra., E-Voting Undermined by Sloppiness* and *Diebold May Face Criminal Charges.*

[38] *Supra., Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting Systems*, at 3-9.

[39] *Supra., Voting Technology in the United States: Overview and Issues for Congress* at 4.

[40] Verified Voting Foundation, *Election 2004 E-voting Incidents from the Election Incident Reporting System (EIRS)*, November 18, 2004, available at http://www.verifiedvoting.org/article.php?id=5321

[41] Press Release, House Committee on the Judiciary, *Government Accountability Office to Conduct Investigation of 2004 Election Irregularities*, November 23, 2004, available at: http://www.house.gov/judiciary_democrats/gaoelectionjtpr112304.pdf .

[42] National Institute for Standards and Technology, *Improving the Usability Accessibility of Voting Systems and Products*, NIST Special Publication 500-256 (May 2004), at iv, available at http://www.eac.gov/docs/finalhfvotereport-4-29-041.pdf ("In general, the **single most critical need** identified in this report is a set of usability standards for voting systems that are performance-based and support objective measures and associated conformance test procedures that can be used for the certification and qualification of voting products and systems.")

[43] The non-partisan Election Protection Coalition consists of approximately 60 nonprofit organizations. See http://www.electionprotection2004.org/

[44] See http://www.verifiedvoting.org/

[45] See http://www.cpsr.net/

[46] See http://voteprotect.org/

[47] We will refer to election incident reports taken from EIRS by their EIRS incident numbers. These numbers can be entered into EIRS' search tool to view incident details: https://voteprotect.org/index.php?display=EIRMapNation&tab=ALL

[48] EIRS: 29656

[49] EIRS: 32535, 29727

[50] EIRS: 47357, 47630, 41092, 39792, 35601

[51] EIRS: 41693

[52] EIRS: 29471, 31377, 32814, 32895, 33406, 33429, 34249, 35050, 35481, 35752, 35862, 36177, 34703, 36180, 36812, 37481, 37666, 37893, 38151, 38543, 37831, 39531, 39505, 38825, 40147, 40410, 40558, 40870, 43872, 42848, 44658, 45403, 45753, 45447, 46394, 46290, 46528, 46762, 46690, 46917, 46968, 46893, 47289, 47376, 47683, 47757, 47873, 47979, 48034, 48073, 48439, 48623, 49209, 49300, 49986, 49950, 50700, 50583, 51167, 51819, 41196

[53] EIRS: 42692, 43999, 39396

[54] EIRS: 43856

[55] EIRS: 46835, 35436

[56] EIRS: 42692, 35105

[57] EIRS: 29471, 34419, 44723

[58] EIRS: 41725, 46108, 47355, 34353

[59] EIRS: 40494, 44481, 44706, 47555, 47570, 47596, 47678, 48599, 48935, 36946, 36750, 34419, 31931, 31061, 29262

[60] EIRS: 50143

[61] EIRS: 39880

[62] EIRS: 51460

[63] A "button-matrix DRE voting machine" is an older type of DRE that doesn't use a touch-sensitive display monitor but instead uses a large, full-face ballot placed over a matrix of buttons. The voter presses their choice on the full-face ballot and this action depresses the button underneath their choice. These machines include the Sequoia AVC Advantage and the Guardian Voting Systems ELECTronic 1242 (a/k/a Shouptronic 1242).

[64] EIRS: 35052, 39433, 41871, 44164, 43856, 48801

[65] EIRS: 33169, 33706, 40402, 33170

[66] EIRS: 47606, 39609

[67] EIRS: 44666, 49261, 45139, 47475, 35310, 51555, 40645, 35052, 33706
[68] EIRS: 29974, 34517, 34581, 39562
[69] This effectively stopped voting for all other voters in the precinct as there are procedural regulations that require a certain number of poll workers inside the polling place while voting is being conducted and two poll workers must accompany the DRE taken to the disabled voter outside the polling place.
[70] EIRS: 38279
[71] EIRS: 40217, 43261, 44943, 45884
[72] Some DREs handle this by specifically not recording the ballot until the "cast ballot" button/choice is pushed. If there is a crash during voting, the voter simply must revote their ballot.
[73] Sequoia's AVC Advantage full-face button-matrix DRE is known to conduct logic and accuracy tests during its boot process but records these votes to an isolated internal memory register. See Sequoia Voting Systems, Inc., *AVC Advantage® Security Overview*, Oct. 2004, at 7 (on file with author).
[74] Recalibration of a touchscreen involves poll workers using a computer program that prompts them to touch a few pre-programmed places on the screen to allow the system to adjust where it registers the user is touching. If a touchscreen is poorly calibrated, touching the screen on one part of the screen will be interpreted by the system as being a touch in a different part of the screen.
[75] *Supra.*, *Improving the Usability Accessibility of Voting Systems and Products*, at 56. ("6.10.1 Develop a valid, reliable, repeatable, and reproducible process for usability conformance testing of voting products against the standards described in recommendation 1) with agreed upon usability pass/fail requirements.")
[76] For example, due to ballot roll-off, the buttons corresponding to presidential choices will be heavily used during a presidential election. ("Roll-off" refers to voters preferentially voting for contests at the top of the ballot.)
[77] Note that HAVA requires that disabled voters be able to cast ballots independently and in private. See §§ 42 USC 15481(a)(3)(A) (voting systems shall provide equal opportunity for access and participation of disabled voters including privacy independence)
[78] *Supra.*, *Improving the Usability Accessibility of Voting Systems and Products*, at 55. ("6.8.1 Encourage vendors to incorporate a user-centered design approach into their product design and development cycles including formative (diagnostic) usability testing as part of product development.")
[79] Only in cases where ballots are physically mangled or otherwise rendered unascertainable to the human eye are paper-based tabulation errors unrecoverable.
[80] §§ 42 USC 15481(a)(2) (Requiring that voting systems allow voters to change their vote and that they produce a permanent paper record of the vote that should be available in recount proceedings.)
[81] *Supra., Auditing Elections*, at 49.
[82] *More Than 4,500 North Carolina Votes Lost Because of Mistake in Voting Machine Capacity*, Associated Press / USA Today, November 5, 2004, available at http://www.usatoday.com/news/politicselections/vote2004/2004-11-04-votes-lost_x.htm

[83] David Ingram, *NC Ballot Count Could Bring Revote*, Winston-Salem Journal, November 19, 2004, available at http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1031779235637

[84] John McCarthy, *Machine Error Gives Bush 3,893 Extra Votes in Ohio*, Associated Press / USA Today, November 6, 2004, available at http://www.usatoday.com/tech/news/techpolicy/evoting/2004-11-06-ohio-evote-trouble_x.htm

[85] Binyamin Appelbaum, *Gaston Investigates Election Tally Errors*, The Charlotte Observer, November 16, 2004, available at http://www.charlotte.com/mld/observer/news/local/10192340.htm?1c

[86] *Discrepancies Found In Numbers Of Gaston Votes, Voters*, Associated Press / Raleigh Durham News Observer, November 18, 2004, available at http://newsobserver.com/news/ncwire_news/story/1839095p-8157912c.html

[87] Richard Rubin and Carrie Levine, *County Retallies Early-Vote Results*, The Charlotte Observer, November 4, 2004, available at http://www.charlotte.com/mld/charlotte/news/politics/10094165.htm

[88] *Supra., Voting Systems Standards (2002)*, Volume I, § 6.5.2, at 6-9.

[89] *Supra., List of Voting Systems that are NASED Qualified.*

[90] *Broward Vote-Counting Blunder Changes Amendment Result*, WJXT, November 4, 2004, available at http://www.news4jax.com/politics/3890292/detail.html

[91] Kevin Connolly, *Computer Glitches Slow Volusia Results*, Orlando Sentinel, November 4, 2004, available at http://www.orlandosentinel.com/news/elections/orl-asecvolusiaglitches04110404nov04,1,3289659.story .

[92] Kori Kamradt, *Voter Turnout Still Not Known*, LaPorte County Herald-Argus, November 4, 2004, available at http://www.heraldargus.com/content/story.php?storyid=5304

[93] Antone Gonsalves, *San Francisco Finds Fix For Election Day Tech Snafu*, InternetWeek.com, November 5, 2004, available at http://www.internetweek.com/allStories/showArticle.jhtml?articleID=52200321

[94] *Recount Changes One Franklin Co. Race*, Associated Press, November 12, 2004, available at http://www.indystar.com/articles/0/194113-4600-102.html

[95] Tad Walch, *Utah County Votes Counted Incorrectly*, Desert Morning News, November 14, 2004, available at http://deseretnews.com/dn/view/0,1249,595105309,00.html

[96] If the hardware remains unchanged, it does not have to be recertified. If it does change, it must be recertified against the 2002 VSS, which would be quite difficult given the heightened requirements. Counties can continue to use these systems past the January 1, 2006 deadline for implementing HAVA's mandatory minimum requirements (see, §§ 42 USC 15481(a)(1)-(6)) if they provide one accessible DRE per polling place (see, § 42 USC 15481(a)(3)(B)).

[97] Federal Election Commission, *Known Vendors of Computerized Vote Tabulation Systems,* December, 7, 2000, available at http://www.fec.gov/pages/vendors12-00.htm

[98] See discussion of the Avante Vote-Trakker and Diebold AccuVote-TSx, *supra.*, note 13.

[99] See extended discussion in, *supra., Improving the Usability Accessibility of Voting Systems and Products*, and Benjamin Bederson and Paul Herrnson, *Usability Review of the Diebold DRE System for Four Counties in the State of Maryland,* University of Maryland, (2002), available at http://www.capc.umd.edu/rpts/MD_EVoteMach.pdf

[100] *Supra., Auditing Elections,* at 46. ("As with financial auditing, an audit can be initiated in response to suspicion of impropriety, but auditing is at its most effective as a deterrent to fraud and error if it is also conducted routinely.")