Trust but Verify

X

Increasing Voter Confidence in Election Results

Staff Report
2007

TACIR
Publication Policy

Staff Information Reports, Staff Briefs, Staff Technical Reports and Staff Working Papers and TACIR Fast Facts are issued to promote the mission and objectives of the Commission. These reports are intended to share information and research findings relevant to important public policy issues in an attempt to promote wider understanding.

Only reports clearly labeled as "Commission Reports" represent the official position of the Commission. Others are informational.

Trust But Verify

Increasing Voter Confidence
In Election Results

Prepared by:

Harry A. Green, Ph.D.
Executive Director

❖

Rose Naccarato, Ph.D.
Senior Research Associate
Author, Project Management

❖

Reem Abdelrazek, M.P.A.
Research Associate

Other Contributing Staff:

Teresa Gibson
Web Development & Publications Manager

Ken Belliveau, M.C.P, A.I.C.P.   Cliff Lippard, M.P.A.
Catherine Corley, M.A.   Daniel Merchant, M.S.
Kerri Courtney, M.P.A.   Lynnisse Roehrick-Patrick, J.D.
Leah Eldridge, J.D.   Beth Swartz, Ph.D.
Sallie Hussey, M.A.   Libby Thurman, M.A.
David Lewis, M.A.   Ed Young, Ph.D.

Staff Report
2007

TABLE OF CONTENTS

PURPOSE

In December 2006, the Tennessee Advisory Commission on Intergovernmental Relations voted to review the entire election process, including an examination of the advantages and disadvantages of voting machines currently used in Tennessee. This, the first report to result from that review, focuses on issues related to voting machines because any changes to voting systems will take time to implement. Subsequent reports will examine other aspects of the electoral process, including ensuring voter eligibility and regularly auditing compliance with election rules and procedures.

EXECUTIVE SUMMARY

With talk of amending the Help America Vote Act (HAVA) and the possibility of additional federal funds to implement voter verified paper audit trails (VVPAT) for the 2008 or 2012 presidential elections swirling about, Tennessee's local election commissions once again face the possibility of changing their voting systems. This may be a good thing. Many voters and experts lack confidence in the machinery and process of elections despite the replacement of voting systems all across the country. Tennessee has not been immune. A group of voters in Memphis and Shelby County were sufficiently concerned to hire an elections expert to review reports of problems there and remain distrustful of the system.

There are no formal requirements or methods for reporting voting problems in Tennessee or nationally. At every election, some reports of problems appear in the press, and there are organizations that gather those press reports and make them available to the public. Such lists are useful but can by no means be considered complete. A March 2007 Government Accountability Office (GAO) study found that improvement was needed at all levels of government. Specifically, the report found inadequacies in national standards, system design and development, operation and management activities, and testing. Additionally, the report cited wide variances in state and local standards, including types of testing that are not commonly performed.

Tennessee is one of only 20 states that requires neither a voter verified paper audit trail (VVPAT) nor a routine post-election audit. Eight of those 20 states have VVPAT statewide, though it is not specifically required. Despite the concerns expressed by voters, only 15 states require both, and 15 more require some form of VVPAT, but no post-election audit.

Two bills in the U.S. Congress are currently under consideration that would require paper trails, the "Voter Confidence and Increased Accessibility Act of 2007" (also known as the "Holt bill") and the "Ballot Integrity Act of 2007" (also known as the "Feinstein bill"). Even if Congress does not amend HAVA and

> There are no formal requirements or methods for reporting voting problems in Tennessee or nationally.

fund VVPAT, Tennessee may wish to address the concerns of voters on its own. This report, an early release on a broader study of election reform issues authorized by the Tennessee Advisory Commission on Intergovernmental Relations (TACIR) in December 2006, focuses on VVPAT because implementation of changes in voting technology require more time than other reforms. We hope that this report, as well as the broader study, will be of assistance to the special joint committee established by SJR 745 (formed to study the Tennessee Voter Confidence Act of 2006).

VOTING MACHINES

The lack of voter verification is certainly not new. Though the earliest American elections made use of voice votes recorded on paper by multiple observers and paper ballots, the first mechanization of elections relied on lever machines. These machines could be easily manipulated by turning dials in the back, and their vote records were notoriously unreliable even when used correctly. With years of storage between uses, the gears that counted the votes could become sticky and rusted and affect the vote count.

Computer-read ballot systems first appeared in the 1960s and began quickly to displace mechanical systems. Voters either punched a card or used a No. 2 pencil to mark a standardized form; both could be read by a person or a computer. Computer touch screens and direct recording electronic (DRE) machines were first introduced in the 1990s and have been used by some Tennessee jurisdictions now for more than a decade. Most states now use optical scan machines, DREs, or some mixture of the two, though a number of counties in ten states still use hand-marked, hand-counted paper ballots.

Both optical scan machines and DRE machines supplemented by DRE printers can produce a VVPAT. For both types of paper record balloting, the massive amount of paper that must be handled by poll workers raises security issues. Paper can be damaged, lost, mishandled, or stolen. Furthermore, both kinds of machines are subject to hacking and software tampering to

Paper trails reassure voters that their vote is being counted accurately and can be audited or recounted.

change vote totals. But even so, paper trails reassure voters that their vote is being counted accurately and can be audited or recounted.

DIRECT RECORDING ELECTRONIC VOTING MACHINES

DRE machines present voters with candidates and issues on a computer screen or a succession of screens. Voters choose their candidate by pressing a button, touching the screen, or turning a dial. DREs are thought to decrease voter error because they generally ensure against over-voting (voting for more than one candidate in a race) and decrease the likelihood of under-voting (not voting in a race) by offering the voter a summary screen for their review. Allowing voters to check their ballots on the screen before submitting them also may reduce voter error. Despite these advantages, many experts and advocates believe that DREs are especially vulnerable to tampering and fraud, mainly because most do not physically document individual votes so that they can be independently recounted or audited.

Vulnerability in all electronic or computerized systems can stem from computer codes that are subject to tampering, connections to other computers that can allow hacking, and weak data encryption. In addition to being vulnerable to tampering and fraud, DREs, like the old lever machines and computerized paper-ballot readers, are subject to mechanical malfunction. And when there is no actual paper vote, detecting malfunction and fraud is more difficult. To detect these problems and safeguard against them, some propose having DREs produce a paper ballot for voters to verify their choices and for local election officials to retain a record of the vote. This is generally known as a voter verified paper audit trail or VVPAT.

VVPAT is a feasible option with DREs, while it was not with lever machines. VVPAT can also help to guard against the new opportunities for fraud that DREs present: altering the vote count on a widespread basis and doing so from a remote location.

> Many experts and advocates believe that DREs are especially vulnerable to tampering and fraud because most do not physically document votes so that they can be independently recounted or audited.

OPTICAL SCAN MACHINES

Optical scan systems require voters to record their selections on a paper ballot by filling in a small circle or arrow located next to the candidate of their choice. They can record write-in candidates on the same ballot. After the voter has filled out his or her ballot, it is fed into an optical scanning device that reads the voter's choices and records the votes electronically.

Optical scan systems come in two varieties: precinct-level and centrally-tabulated. Precinct-level systems allow the voter to feed the ballot into the counting machine after completing it. If the voter has voted for more than the allowed number of candidates or has written in a candidate name that cannot be read by the scanner, the scanner will not accept the ballot, and the voter is given an opportunity to correct the ballot. Once read by the scanner, the ballot is stored in the scanning device until it is unlocked and opened up by approved election personnel.

Centrally tabulated optical scan systems have a smaller number of counting machines at a central location where all ballots are tallied after the polls have closed. While voters can still correct a faulty ballot with this system, they must notice the ballot problem themselves. With the precinct-level option the tabulating machines can recognize and alert the voter to several common errors. Most new optical scan voting systems are precinct-level ones.

One of the main differences between optical scan systems and DREs with VVPAT is that, while both have paper records, the DRE with VVPAT record was created by the computer, using the same software that counted the votes. The optical scan paper record is marked by the voter herself.

POTENTIAL IMPROVEMENTS FOR TENNESSEE ELECTIONS

After reviewing what is known about voting machines, as well as practices in Tennessee and other states, TACIR staff suggests the following possible changes:

✓ **Implement voter-verified paper audit trails statewide within a reasonable time frame.** Distrust of voting systems that are entirely electronic is widespread, undermines voter

The DRE with VVPAT record is created by the computer, using the same software that counts the votes. The optical scan paper record is marked by the voter.

No requirements are under serious consideration in Congress that would preclude the use of precinct-level optical scan systems.

confidence, and may discourage voting. The current system allows no check of the electronically-generated count other than one that uses the same machines and software to recount the same electronically recorded votes. Though recounts of DRE totals sometimes uncover votes that went uncounted for various reasons, they do not include a count that is independent of the voting machines. If something unusual happens in the election, especially if it involves some kind of equipment malfunction, voters are simply unsatisfied if there are no physical ballots to recount. Current VVPAT alternatives include optical scan machines and supplementing DRE machines with DRE printers.

Studies have repeatedly shown that optical scan systems have lower up-front costs than DREs, but that ballot printing costs may make DREs the less expensive option if they remain in use beyond about 20 years. Other studies have refuted the idea that DREs ever become cost-competitive with optical scan systems, showing that DREs do not last for 20 years and that many more DREs per precinct are required compared to optical scan counting machines to provide adequate access to voters.

✓ **Adopt VVPAT that can be counted by hand, as well as by machine—machine tallies to support prompt reporting of results with hand counting for audit and recount purposes.** Experience thus far with attaching printers to DREs has been unsatisfactory, mainly because of readability. Vendors are working on better systems, but they are still in the planning and experimental stages. If DRE printers are adopted, care should be taken to ensure that they will support hand counting. Hamilton and Pickett Counties currently use optical scan systems countywide for most voters and have DREs for disabled voters. Ballot marking devices that can be used by disabled voters to mark their optical scan ballots in privacy, print them, and put them in the ballot boxes like all other voters are available.

✓ **Adopt a standard for VVPAT that would meet federal guidelines under consideration.** While staff concludes that waiting for Congressional action is not advisable, it would be unwise to ignore the standards likely to emerge if Congress passes a bill. These standards cannot currently be met by DRE printers. If such printers were purchased and Congress passed the "Holt bill" or the "Feinstein bill," the new printers would have to be discarded. No requirements are under serious consideration in Congress that would preclude the use of precinct-level optical scan systems.

✓ **Request a review by the Election Assistance Commission to find out how much of Tennessee's remaining HAVA funds would be available to purchase new voting machines.** When Florida's current Governor Charlie Crist asked the state legislature to require optical scan machines in all precincts in the state, he requested that the EAC allow him to spend some of Florida's remaining HAVA funds on the change. In a written response, Juliet T. Hodgkins, General Counsel for the EAC, stated that counties which had already used HAVA funds to replace their voting machines could not do so again. The EAC review found that some of Florida's HAVA funds could be used, but the reasons were very situation-specific. Tennessee should request a similar review so the state knows the full funding situation.

✓ **Require voting machine vendors to escrow all of their proprietary software so that it can be reviewed by experts as recommended by the Commission on Federal Election Reform and secured for further analysis <u>if vote-counting problems should arise</u>.** The inability to study the software when there are questions about an election with no paper records seriously undermines confidence in the results of recounts and audits. Elections are the basis of democracy, and it is not acceptable for a private interest to shield a part of the election process from the voters those private interests serve. Taxpayer dollars buy the voting machines and the software, and taxpayers have the right

Governmental entities and private corporations are routinely audited regardless of whether problems are suspected. With so much at stake, the same should be true for elections.

to ensure that their investment will produce reliable results. The source code is the actual counter of votes, and that counting must be more open if the public is to accept close election outcomes. Vendors may have valid concerns about proprietary software, and those concerns should be addressed as much as practicable, but at the very least, source code must be available for inspection by someone who is not in the vendor's employ when an election is close and in question. Inspectors could be limited to a small number of qualified people, and they can be required to sign non-disclosure agreements. Having a copy of the source code as delivered by the vendor would provide protection to vendors as well. In the event that the code was altered after delivery, vendors would have an official record of the code as they delivered it. A process that would allow for open examination of source code is desirable and should be explored for the future. One possibility is using voting machines with all open source code programs.

✓ **Strengthen audit requirements to ensure that a random sample of machines is routinely tested by comparing hand counts to machine totals, and when results vary by more than a small percentage, that a broader recount process follows.** Numerous studies have demonstrated that machine counters can be programmed, maliciously or negligently, to miscount. Small miscounts might not create enough suspicion to prompt a recount, especially in a statewide or national race in which individual counties do not get much notice. But systematic small miscounts can change the outcome in any close race. Governmental entities and private corporations are routinely audited regardless of whether problems are suspected. With so much at stake, the same should be true for elections.

In most states that require audits, a small number of precincts are randomly chosen to recount their ballots fully. Any discrepancies are investigated. If satisfactory explanations cannot be found, then all precincts will recount. Some states randomly select a percentage of

In Tennessee, nearly 50% of the statewide November 2006 vote was cast early.

ballots in all precincts and recount them manually. Any recount totals that do not fall within a specified margin of error for the overall precinct total trigger a wider recount. As an alternative, several states have an automatic partial or full recount only when a race is very close (generally when the top two candidates are within a point or two of each other). The State of Minnesota enacted a post-election review law in 2004 to assess the accuracy of its voting machines. If the audit reveals a difference greater than 0.5%, a broader audit is automatically triggered.

✓ **Consider making early voting and voting by mail more accessible.** Broadening the availability of both would reduce the pressure on polling places on election day, addressing one of the concerns of recent elections—long lines and long waits. Voting early has proven quite popular where it is widely available. In Tennessee, nearly 50% of the statewide November 2006 vote was cast early. Some Tennessee legislators have reported receiving complaints about the lack of access to early voting by those outside of cities. It should be a real option for rural voters as well as for urban ones. More locations and a longer early voting period are options to consider. Voting by mail is essentially absentee voting. Tennessee requires a reason for voting absentee. Most states do not. Allowing anyone who wishes to vote absentee would increase voting opportunities. There is reason to believe it would increase voter turnout while taking some of the pressure off of polling places that can result in long lines on election day.

✓ **Consider a Vote by Mail pilot program that would allow the state to assess the advantages and disadvantages of this type of voting in Tennessee.** The success and acceptance of voting by mail in states like Oregon and Washington suggests that it is worth further investigation. Voting by mail creates its own paper trail, solving the problem most DREs pose for recounts and audits, but it may create other problems. Potential benefits include decreased expense and higher turnout. In Tennessee, the Joint Study Committee on the Voter Confidence Act of

In Tennessee, the Joint Study Committee on the Voter Confidence Act of 2006 recommended a Vote by Mail pilot program.

2006 recommended a pilot program, and a bill currently in Congress would fund such a program if it passes. Given the potential to increase voter turnout, a pilot program in Tennessee might be desirable regardless of whether federal funding becomes available.

✓ **Strengthen security and pre-test requirements and make them consistent for all voting systems.** The testing requirements for different types of voting systems are not consistent, and there is much that is out-of-date and no longer applies. While this is not necessarily critical to fair elections, it does need to be done at some point.

✓ **Consider election day parallel voting machine tests to detect hidden programs that are triggered by election day conditions and are erased so that they cannot be detected later.** Several jurisdictions, including at least one state, choose voting machines at random on election day, remove them from use, put them on public display, and use them to test the equipment and software to ensure that nothing that happens during the day affects vote counts. A series of predetermined ballots are cast on the test machines periodically throughout the day; totals for each machine are checked at the end of the day to make sure all ballots were counted correctly. These tests measure the election day performance of the machines and ensure that they do not have hidden programs that activate only on election day and cause miscounts. The State of Maryland used this process in 2004, casting 1,300 ballots to test the reliability of their machines. If optical scan were to be adopted statewide, most counties would have only one counting machine per precinct. Parallel tests could still randomly select at least one machine per county to test openly on election day.

INTRODUCTION

Americans want a voting system that is private, secure, and accurate to decide issues and elect our nation's leaders. Concern that the system we have falls short came to a head following the 2000 presidential election, which ended only when the U.S. Supreme Court halted recounts in Florida more than a month after the polls had closed. Despite the broad overhaul of voting systems that has taken place with funding from the federal Help America Vote Act (HAVA) passed by Congress in 2002, several recent elections have highlighted continued problems with voting technology and procedures, and many voters remain concerned. A 2006 Zogby poll[1] of likely voters found that

- 61% are aware that there have been reports of flaws in electronic voting machines that make it possible to tamper with one machine in such a way as to change the results of an entire election,

- 80% believe that it is unacceptable for votes to be counted in secret without any outside observers from the public, and

- 92% feel that citizens have a right to view and obtain information about how election officials count votes.

Many experts argue that the use of a voter verified paper audit trail (VVPAT) or a post-election audit improve election security and accuracy. Tennessee is one of only 20 states that will require neither a VVPAT nor a routine post-election audit in 2008. Eight of those 20 states have VVPAT statewide, though it is not specifically required. Despite the concerns expressed by voters, only 15 states require both VVPAT and a post-election audit, and 15 more require some form of VVPAT, but no audit.

Tennessee is one of only 12 states that will not have statewide voter verified paper audit trails (VVPAT) in 2008.

By the November 2006 general election, only New York and Idaho retained any of the older voting technologies.

BACKGROUND

The lack of voter verification is certainly not new. Though the earliest American elections made use of voice votes recorded on paper by multiple observers and paper ballots, the first mechanization of elections relied on lever machines. These machines could be easily manipulated by turning dials in the back, and their vote records were notoriously unreliable even when used correctly. With years of storage between uses, the gears that counted the votes could become sticky and rusted and affect the vote count.

Computer-read ballot systems first appeared in the 1960s and began quickly to displace mechanical machines. Voters either punched a card or used a No. 2 pencil to mark a standardized form; both could be read by a person or a computer. Computer touch screens and direct recording electronic (DRE) machines were first introduced in the 1990s and have been used by some Tennessee jurisdictions now for more than a decade.

By the November 2006 general election, only New York and Idaho retained any of the older voting technologies. New York's remaining lever machines are scheduled to be replaced in time for their September 2007 elections, and 12 of the 13 remaining punch-card counties in Idaho are in the process of converting to optical scan. The last county, Bonneville, is trying to keep the punch-card system its voters are fond of, but there is only one technician left in the country, and services such as ballot printing are becoming increasingly hard to find.[2]

Most states now use optical scan machines, DREs, or some mixture of the two, though a number of counties in ten states still use hand-marked, hand-counted paper ballots.

DIRECT RECORDING ELECTRONIC VOTING MACHINES

DRE machines present voters with candidates and issues on a computer screen or a succession of screens. Voters choose their candidate by pressing a button, touching the screen, or turning a dial. DREs are thought to decrease voter error because they generally ensure against over-voting (voting for more than one

candidate in a race) and decrease the likelihood of under-voting (not voting in a race) by offering the voter a summary screen for their review. Allowing voters to check their ballots on the screen before submitting them also may reduce voter error. Despite these advantages, many experts and advocates believe that DREs are especially vulnerable to tampering and fraud, mainly because most do not physically document individual votes so that they can be independently recounted or audited.

Vulnerability in all electronic or computerized systems can stem from computer codes that are subject to tampering, connections to other computers that can allow hacking, and weak data encryption. In addition to being vulnerable to tampering and fraud, DREs, like the old lever machines and computerized paper-ballot readers, are subject to mechanical malfunction. And when there is no actual paper vote, detecting malfunction and fraud is more difficult. To detect these problems and safeguard against them, some propose having DREs produce a paper ballot for voters to verify their choices and for local election officials to retain a record of the vote. This is generally known as a voter verified paper audit trail or VVPAT.

VVPAT is a feasible option with DREs, while it was not with lever machines. VVPAT can also help to guard against the new opportunities for fraud that DREs present: altering the vote count on a widespread basis and doing so from a remote location.

OPTICAL SCAN MACHINES

Optical scan systems require voters to record their selections on a paper ballot by filling in a small circle or arrow located next to the candidate of their choice. They can record write-in candidates on the same ballot. After the voter has filled out his or her ballot, it is fed into an optical scanning device that reads the voter's choices and records the votes electronically.

Optical scan systems come in two varieties: precinct-level and centrally-tabulated. Precinct-level systems allow the voter to feed the ballot into the counting machine after completing it. If the voter has voted for more than the allowed number of candidates

> Despite the advantages they offer, many experts and advocates oppose the use of DREs because they believe that DREs are especially vulnerable to tampering and fraud.

> As implemented in many states, including Tennessee, the Help America Vote Act's manual audit capacity does not require a paper record of each voter's selections.

or has written in a candidate name that cannot be read by the scanner, the scanner will not accept the ballot, and the voter is given an opportunity to correct the ballot. Once read by the scanner, the ballot is stored in the scanning device until it is unlocked and opened up by approved election personnel.

Centrally tabulated optical scan systems have a smaller number of counting machines at a central location where all ballots are tallied after the polls have closed. While voters can still correct a faulty ballot with this system, they must notice the ballot problem themselves. With the precinct-level option the tabulating machines can recognize and alert the voter to several common errors. Most new optical scan voting systems are precinct-level ones.

One of the main differences between optical scan systems and DREs with VVPAT is that, while both have paper records, the DRE with VVPAT record was created by the computer, using the same software that counted the votes. The optical scan paper record is marked by the voter herself.

THE HELP AMERICA VOTE ACT

On October 29, 2002, President Bush signed the Help America Vote Act (HAVA) into law imposing a January 2006 compliance deadline on states. According to the National Association of Secretaries of State, states had to

- implement a system that notifies voters if they "over vote" and gives them the opportunity to correct their ballots;

- utilize a voting system that produces a permanent paper record with a manual audit capability;

- provide disability access equal to the level of access, privacy, and independence available to other voters; and

- define uniform standards for what constitutes a vote on each type of voting equipment used in the state.[3]

As implemented in many states, including Tennessee, HAVA's manual audit capacity does not require a paper record of each voter's selections. Instead, it consists of printouts run prior to any

> One of the main differences between optical scan systems and DREs with VVPAT is that the optical scan paper records is marked by the voter.

voting showing that the machines have no votes tallied, and printouts run after the polls close showing the vote totals for each machine. Both sets of printouts are often publicly displayed; in Tennessee such displays are required. DREs also keep an electronic record of each ballot, but these rely on the same electronic count that produces the vote totals. They are not filled out by the voter and are not voter-verified auditable records.

This means that, while the opportunity to review their votes on screen provides voters some degree of confidence that they voted as they intended, it does not ensure that their vote will be recorded and tallied correctly. It also does not allow for machine-independent manual audits or recounts. This particular aspect of electronic voting produces the most concern among critics of those systems.
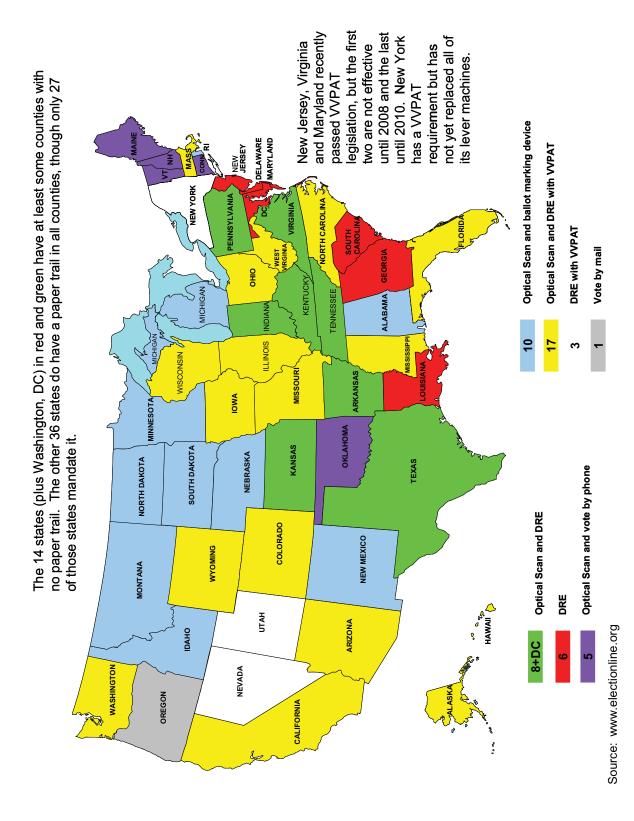
Figure 1 shows the technologies each state uses to vote. Thirty states have already moved to require a paper voting record. In those states, a paper record is presented to voters at the time of voting for their verification. In addition to allowing voters to see what the machine has recorded, the paper records can be summoned if a recount is warranted, and they can be audited manually as HAVA requires. In states without VVPAT, including Tennessee, recounts of DRE votes consist of machines re-tallying the votes as stored. If the votes are stored incorrectly, either because of a machine malfunction or fraud, these "recounts" are useless.

Complying with HAVA generally required states to replace their existing voting technologies, as even the optical scan and DRE machines in place did not usually meet HAVA requirements. Most optical scan systems in use prior to HAVA used central tabulating machines and did not notify voters if they over-voted (chose more options than were allowed for one race or question).* Neither type complied with HAVA's disability access requirements.

---

* HAVA allowed central tabulating optical scan and punch card voting systems to remain as long as disability requirements were met and voter education programs educated voters in over-voting and how to correct their ballots if they over-voted. Lever machines were deemed non-compliant with HAVA, as they had no paper records. Most counties across the country opted to purchase new voting equipment while they had the chance to use federal funds for the purpose.

> In states without VVPAT, including Tennessee, recounts of DRE votes consist of machines re-tallying the votes as stored. If the votes are stored incorrectly, either because of a machine malfunction or fraud, these "recounts" are useless.

FIGURE 1. ELECTRONIC VOTING SYSTEMS IN THE UNITED STATES 2006

The 14 states (plus Washington, DC) in red and green have at least some counties with no paper trail. The other 36 states do have a paper trail in all counties, though only 27 of those states mandate it.

New Jersey, Virginia and Maryland recently passed VVPAT legislation, but the first two are not effective until 2008 and the last until 2010. New York has a VVPAT requirement but has not yet replaced all of its lever machines.

Optical Scan and ballot marking device — 10
Optical Scan and DRE with VVPAT — 17
DRE with VVPAT — 3
Vote by mail — 1

Optical Scan and DRE — 8+DC
DRE — 6
Optical Scan and vote by phone — 5

Source: www.electionline.org

The new DREs and precinct-level optical scan machines do notify voters of over-votes. They also notify a voter if he under-votes (fails to cast a vote in a race or on a question or votes for fewer options than allowed). Under-vote notification is not a HAVA requirement, but according to a special report by Charles Wise of Indiana University it is still a concern to many election commissions.

As a result of HAVA, most jurisdictions across the country opted for one of two types of voting systems. Some chose the new breed of DREs that were more interactive than previous models and could warn voters of ballot problems. These DREs also have audio capacity and other accessibility features that allow voters with disabilities to be guided through the voting process privately.

Other jurisdictions chose precinct-level optical scan systems with at least one other type of machine per precinct that allowed private handicapped access. Such accessible machines included DREs, ballot marking devices (similar to DREs, but they produce an optical scan ballot rather than tallying the vote), and vote-by-phone devices (the voting booth has a telephone in it, on which the voter hears an audio ballot and responds by pressing buttons).
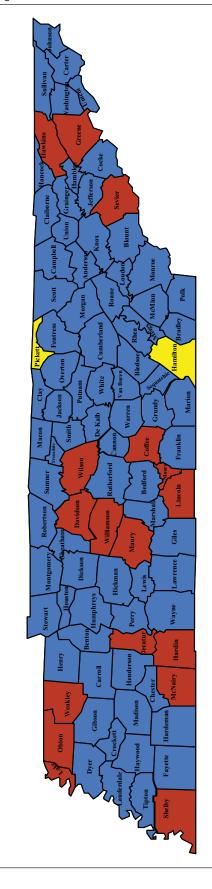
THE POST-HAVA EXPERIENCE IN TENNESSEE

After completing its HAVA plan in 2004, the State Election Commission and the Coordinator of Elections faced the daunting task of getting every county in the state into full compliance with HAVA by the November 2006 general election. They did make that deadline, and all Tennessee counties made use of DREs or precinct-level optical scan machines (with DREs for handicapped access) in November 2006. The types of voting machines now used by each county in Tennessee are shown in Figure 2.

A number of counties were still using punch card and lever machines, and HAVA provided funds to help convert those counties to optical scan or DRE machines. In addition, all Tennessee counties had to be in compliance with the provisions HAVA made for disabled voters, or the state would lose its HAVA funding.

All Tennessee counties made use of DREs or precinct-level optical scan machines (with DREs for handicapped access) in November 2006.

FIGURE 2. TENNESSEE VOTING SYSTEMS

Optical Scan Machines plus Touch Screen DRE's for Handicapped and Disabled Access (Hamilton County uses the Diebold Accuvote and Pickett County uses ES&S)

Touch Screen DRE's (ES&S Ivotronic in all but Shelby County, which uses Diebold Accuvote)

Push Button DRE's (Hart Eslate and Microvote Infinity – Bedford, Carter, Franklin, Hamblen, Marshall and Warren Counties still use the Microvote 464 for most voting, with the Infinity for disabled voter access)

Source: Tennessee Division of Elections

Other than the two counties in Tennessee that use optical scan machines for the majority of voters (Hamilton and Pickett), no Tennessee counties have voting machines that make a paper record of individual ballots as they are cast. Adding a paper trail in the other 93 counties would require additional equipment.

DOCUMENTED DRE PROBLEMS IN TENNESSEE AND OTHER STATES

After the primary elections in August 2006, four losing candidates for various local Shelby County elections asked to see the central tabulator database—a request they had to make in court. They hired Jim March, an election machine investigator from California, to review the records. His report noted numerous security breaches.

- Illegal and uncertified software was present that would allow data transfer on small USB "key chain" devices, hand-editing of vote totals, improper reporting of election results, and remote control of the central tabulator.

- Evidence in the activity log showed repeated failed attempts to use an HTML editor, which would allow manipulation of election reporting results. Successful attempts would not show in the log, so it cannot be known if any attempts succeeded.

- There was no router or firewall protecting the central tabulator, leaving it open to access by any county government official.

- A record of use of Windows programs showed frequent use of Microsoft Access, a database program known to provide opportunity to alter results on Diebold voting machines.

The full report is attached in Appendix A.

DRE voting machine supporters have taken these criticisms point by point and offer a plausible explanation for them other than an attempt to commit election fraud. But each incident points to how the machines *could* be used to manipulate elections. Even if

these irregularities have not affected actual election results, they have diminished the confidence of some of the citizens of Memphis and Shelby County in election outcomes there. And there are no physical ballots for these voters to request to be counted. When DREs are used, losing candidates who believe they should have won, as most losing candidates do, may blame these machines. Rightly or wrongly, such candidates and their supporters may distrust a system that is believed to be so vulnerable to undetectable manipulation.

According to the University of Richmond's Election Reform Information Project, there have been many reports of problems with electronic voting in Tennessee, ranging from

- machines that are completely inoperable,

- ballot programming errors,

- memory chip malfunctions,

- inadequate numbers of voting machines/long lines, and

- missing access cards.

Additional DRE problems reported in other states by the Election Reform Information Project include

- paper jams,

- touch screen misalignment,

- tabulation problems,

- malfunctioning access cards,

- truncated candidate names on summary screens,

- power failure (backup batteries generally worked, though South Carolina had battery problems),

- loss of ballots, and

- problems transferring the votes electronically to the clerk's office for counting.

> Even if documented irregularities have not affected actual election results, they have diminished the confidence of some of the citizens in those outcomes.

And then there are problems like those in Shelby County in 2006, which have unclear effects on outcomes, but which leave some voters with a deep distrust of the electoral process. Many of the problems listed here can apply both to DRE voting machines and to optical scan systems, but optical scan systems have the built-in advantage of supporting hand recounts and post-election audits. DRE machines can be supplemented in various ways to produce paper ballots that can be verified by voters and hand counted by election officials and poll workers, but no such system is currently used in Tennessee.

Though there is no national repository of information on voting problems, many organizations follow local reports and list those that they discover. A comprehensive list from the University of Richmond's Election Reform Information Project included voting-machine-related troubles of varying degrees of severity in 32 states. A tabular summary of their report is included in Appendix B.

At the September 27, 2007 meeting of TACIR, Travis Harold, representing DRE manufacturer Hart Intercivic, acknowledged that sometimes there are problems with DRE machines, but he asserted that there are procedures to deal with these problems, and, as far as they are aware, all votes have been recovered when there is a problem. Jimmy Ries, President of Microvote General Corporation, added that all technologies have their own weaknesses, commenting that optical scan systems still provide the voter no proof that their votes are counted as marked. He also pointed out that the Americans with Disabilities organization is against paper balloting of any kind because it believes it puts their voters at a disadvantage. A summary of the comments of all presenters at the September TACIR meeting is located at Appendix C.

A FEW SPECIAL CASES—FLORIDA, CALIFORNIA AND NEW YORK

FLORIDA

One of the more infamous cases from the November 2006 election was, again, in Florida. After suffering the punch card debacle in 2000, former Florida Governor Jeb Bush signed the Florida

> Many of the problems listed here can apply both to DRE voting machines and to optical scan systems, but optical scan systems have the built-in advantage of supporting hand recounts and post-election audits.

Because of the continued problems with electronic voting machines and the lack of a paper trail, current Florida Governor Charlie Crist pushed for legislation to implement optical scan systems statewide.

Election Reform Act of 2001 banning the use of punch card ballots and requiring either optical-scan or electronic voting systems that have "second chance" technology.* DRE problems in the 2002 Democratic gubernatorial primary in Miami-Dade County left a deep distrust among many Florida voters. The results from Sarasota County in 2006, described below, further eroded some Floridians' faith in their electoral process.

Florida's 13th Congressional district race had an overall under-vote rate (the percentage of voters who left the Congressional race blank) of 2%, but the Sarasota County portion of the district registered an 18% under-vote in the race. The official verdict on these troubles was poor ballot design that made voters miss the race on the computer screen, but the inability of the losing candidate to get a meaningful recount or examine the proprietary voting software greatly increased distrust of DREs among some voters.

Because of the continued problems with electronic voting machines and the lack of a paper trail, current Florida Governor Charlie Crist pushed for legislation to implement optical scan systems statewide. He signed the legislation in May 2007, appropriating nearly $28 million to replace Florida's DREs, leaving just enough of the touch screen machines to comply with HAVA's disability requirements.

Following that decision, Sarasota County again became a focus after an HDTV report by Dan Rather, *The Trouble with Touch Screens*. The Rather report stated that the ES&S machines in use in Sarasota County were manufactured in Manila and interviews with workers in the Manila factory revealed that about 40% of the touch screens were rejected for quality control issues. Technical documentation revealed that the company producing the ES&S screens had been warned internally that their process for making the touch screens left them vulnerable to failures in hot and humid weather. The Rather report stated that these same screens were used in Sarasota County in 2006.

---

* Such technology notifies the voter of common ballot problems and gives him or her the chance to fix the ballot.

Questions about the functioning of the machines that were thought to be settled have been raised again, and the federal Election Assistance Commission (EAC), which oversees HAVA implementation and compliance, has requested an accounting from ES&S for its failure to disclose its use of the Manila assembly facility in its EAC certification information.

In a press release available on its website, ES&S has responded to the Rather report, pointing out that its Manila facility met widely recognized international standards, that its equipment testing was more consistent and rigorous than described, and that it eventually replaced all of the touch screens that may have been affected. The company also stated that its failure to disclose the facility to the EAC was an oversight that has been rectified.

CALIFORNIA

California's Secretary of State, Debra Bowen, campaigned on the issue of reforming the state's electoral process. Upon taking office, she instituted a top-to-bottom review of the state's voting machines that began with decertification of all of the machines, to be followed by a full review of each and recertification if warranted. The state contracted with the University of California to conduct the reviews in four areas:

- documents and studies associated with each voting system

- source code in use for each voting system

- a "red team penetration attack" to see if the system can be compromised

- accessibility of the system for disabled voters

The cost of the top-to-bottom review is to be paid using some of California's HAVA funds and by the voting machine vendors.

Security flaws were found in all of the voting systems in California. The "red team penetration attack" tests, essentially attempts by hackers to violate system security, found a way into every system.

According to the published results, California worked with four voting machine vendors prior to the review: Diebold (now Premier

In California Secretary of State Debra Bowen's "top-to-bottom review" of the state's voting machines, security flaws were found in all of the voting systems in use. The "red team penetration attack" tests, essentially attempts by hackers to violate system security, found a way into every system.

The California top-to-bottom review has been closely watched by officials in other states as well. The Secretaries of State in Colorado and Ohio have announced plans to conduct similar reviews in their states.

Election Solutions), Hart InterCivic, Sequoia, and ES&S. ES&S expressed reservations about the University of California reviewers, and it balked at providing its source code. The company finally agreed to do so only after Secretary Bowen formally requested a copy from the facility where it was held in escrow. In the end, Secretary Bowen declared that ES&S had not cooperated fully in a timely fashion and decided not to recertify the ES&S voting machines for future use in California.

The only Direct Recording Electronic (DRE) voting machine approved for future general use in California was the Hart InterCivic System 6.2.1. Some additional security measures were required, as well as extensive post-election audits, but the system was approved. Hart withdrew its system 6.1 from consideration and submitted the new system instead. Premier (formerly Diebold) and Sequoia DREs are to be used in a limited fashion, with just one machine per polling place for disabled voter access. They face strict security measures, including an assigned poll worker to monitor them constantly.

All of the optical scan voting machines submitted for review will be recertified with additional security and post-election audit requirements. A copy of the Frequently Asked Questions (FAQ) document from the California Secretary of State's website is attached at Appendix D.

The California top-to-bottom review has been closely watched by officials in other states as well. The Secretaries of State in Colorado and Ohio have announced plans to conduct similar reviews in their states. Kentucky's Attorney General, after a rather public argument with the Secretary of State, recently launched an investigation that found that the Premier DREs in use in Jefferson County were not certified by the state. Though they had been certified in the past, the state had certified a newer version and the old ones had never been upgraded.

NEW YORK

New York has lagged behind the rest of the nation in updating its voting technology, with much of the state still using outdated lever machines. All states receiving HAVA funds were supposed to be

in compliance with the provisions of the Act in time for the November 2006 election. New York has missed the extended deadline it had been granted under a Consent Decree by the U.S. Department of Justice. It is unclear if there will be consequences for New York or if the state will receive another judicial reprieve, but it could face the loss of most or all of its HAVA funds.

In 2006, New York contracted two independent companies, CIBER and NYSTEC, to test voting machines. Previously, CIBER has approved machines in other states that were later decertified due to equipment and software defects and NYSTEC has been critical of CIBER's security test plan. Indeed, CIBER recently lost its accreditation from the EAC. CIBER did not inform the state election board of its EAC status; it was only brought to light after it was reported in a *New York Times* article. After censure from the state board, CIBER was suspended from any further New York testing in January 2007.

The state election board is currently inspecting machines but has not made any decisions, and the process continues to move slowly. As a result, some New York counties have opted to use uncertified machines in local elections. In May 2007, the City School Board of Troy used LibertyVote DREs for its elections, which are not certified for use in the state of New York. Liberty Election Systems offered the full-face touch screen machines to the city free of charge. The Troy School Board decided that state certification was not necessary for a strictly local election.

Despite lagging on machine updates, New York has passed legislation requiring independent security reviews of voting machine source code. In the case of compromised security, third-party escrowing allows for the underlying software codes used in voting machines to be inspected by an independent third party. Late in the state's 2007 legislative session, Microsoft lobbyists pressed for an amendment to weaken the third-party escrow clause and keep the underlying codes secret (many voting machine vendors use a Microsoft operating system, including Avante and Sequoia). The legislature did not pass the amendment and kept its strict election laws intact.

> In the case of compromised security, third-party escrowing allows for the underlying software codes used in voting machines to be inspected by an independent third party.

SCOPE OF THE STUDY

A recent GAO study found inadequacies in national standards, system design and development, operation and management activities, and testing. Additionally, the report cited wide variances in state and local standards, including types of testing that are not commonly performed.

A March 2007 Government Accountability Office (GAO) study found that improvement was needed at all levels of government. Specifically, the report found inadequacies in national standards, system design and development, operation and management activities, and testing. Additionally, the report cited wide variances in state and local standards, including types of testing that are not commonly performed. While this report focuses on issues related to voting machines, subsequent reports will examine other aspects of the electoral process, such as those identified by GAO, to include ensuring voter eligibility and regularly auditing compliance with election rules and procedures.

Bills introduced in the last session of the Tennessee General Assembly that are relevant to this first report are discussed at the end of each section. Also, attention will be given to three areas depending on the balance of election issue priorities.

- Access vs. Security—ensuring that all eligible voters are able to vote with ease and confidence while ensuring that only those who are eligible to vote are allowed to do so

- Privacy vs. Verifiability—protecting the privacy of voters, so that no one else has the opportunity to see how an individual has voted, while allowing voters to verify that their votes are accurately counted

- Expense vs. Accuracy—balancing the need for accuracy against the expense of attaining it. Some degree of *random* error may be acceptable if the cost of eliminating it is too high

VOTER VERIFIED PAPER BALLOTS AND AUDIT TRAILS

The call for voter verified paper ballots and physical audit trails has been around as long as there have been DRE voting machines. The concept goes by several names, including verified paper record (VPR), voter verified paper ballots (VVPB), and voter verified paper audit trail (VVPAT). The machines that implement these systems take several forms, but in all cases, they offer voters a chance to verify paper copies of their votes. Voters do not remove these paper copies, and they can be retained for hand recounts or audits of an election.

Optical scan voting inherently includes a paper record. While machines tally the votes, optical scan ballots are retained and are the official ballots of record. They can be used to audit the tabulated totals, and they can be used for full manual recounts if necessary.

DREs do not necessarily offer the same paper record. In 12 states (and the District of Columbia), including Tennessee, only an electronic record will exist of voter ballots cast on DREs in 2008. Many of the states with VVPAT have a system that displays the printout behind a transparent window to protect the paper against damage and ensure that it is not removed from the voting area. In some states with these systems, the electronic record is the official ballot record; in others, the paper record is the official one. In the latter case, recounts and audits require use of the printed ballot records.

Printers attached to DREs have thus far been of varying quality and reliability. Printer jams have been common enough to raise questions about the fairness of making the paper ballot the ballot of record. Clear procedures for generating a usable paper ballot for a voter who experiences a printer jam have not been established. In addition, the printers currently in use utilize rolls of thermal paper, like cash register receipt tape. According to computer security expert Dan Wallach, in his testimony in a Colorado court case, type begins to smear and fade on this type of paper in a relatively short period of time, especially if the paper

> Voter verified paper audit trails offer voters a chance to verify paper copies of their votes, and those copies are retained as a physical record that can be used to support a hand recount or audit of an election.

is handled , as it would be in a recount. These records cannot be maintained permanently. Some vendors refute this claim. Furthermore, the large roll does not separate the ballots, which can make recounts very difficult, as well as put the voters' anonymity at risk by keeping records in the same order that voting took place.

If the electronic vote is the ballot of record, then the paper version serves no purpose other than to be verified by the voter. There is little value to this beyond a false reassurance to the voter, as malfunctions and malicious programming can change the electronic count so that it does not match what was printed. If the paper ballots are not the ballot of record, then they do not serve a purpose other than to give the voter something to look at and likely are not worth the cost.

THE COST OF ADDING A PAPER TRAIL

It is possible to reduce some of the costs associated with voter verified paper audit trails by taking other steps to reduce pressure on polling places on election day, such as increased early and absentee voting opportunities.

Studies have repeatedly shown that optical scan systems have lower up-front costs than DREs, but that ballot printing costs may make DREs the less expensive option if they remain in use beyond about 20 years.[4] Other studies have refuted the idea that DREs ever become cost-competitive with optical scan systems, showing that DREs do not last for 20 years and that many more DREs per precinct are required compared to optical scan counting machines to provide adequate access to voters.

Several bills introduced in the last General Assembly include a fiscal note that was based on adding printers to the DREs currently in use in 93 counties. That was estimated as a one-time $9.5 million expense.

None of the bills was interpreted to mean replacing the DREs with optical scan machines, though the State Election Coordinator's office made a rough estimate of a one-time $25 million expense, with unestimated ongoing costs due primarily to ballot printing. This estimate was based on $10,000 to purchase one optical scan ballot counter and one automatic ballot marking device per precinct. The latter is for disability access. It is essentially a DRE that prints an optical scan ballot rather than counting the vote.

In testimony before the Elections Subcommittee of the Congressional Committee on House Administration, Warren Stewart, Policy Director of VoterTrustUSA, gave similar cost estimates of $10,000 per precinct for both an optical scan tabulator and a ballot marking device. He further explained that those machines cost about $5,000 each.

Tennessee has 2,500 precincts and almost 150 of those in Hamilton County and in Pickett County already have optical scan machines. An estimate that is a little less rough would be $12 million to purchase an optical scan machine for each of the roughly 2,300 precincts that lack them and $12.5 million to purchase automatic ballot marking devices for all counties (Hamilton and Pickett Counties currently use DREs for disability access). It would also be possible to do as Florida has done and maintain one DRE per precinct for disability access, allowing the total change to take place for about $12 million.

Adding a paper trail of any kind will, of course, add the cost of paper and its storage. The differences between the two systems on paper costs are not as clear. Thermal rolls may use less storage space, but, unlike optical scan ballots, they require controlled climates. Thermal paper rolls are certainly less expensive to purchase than are printed ballots.

A North Carolina study showed that the additional costs associated with maintaining so many more voting machines and printer attachments in counties using DRE machines resulted in higher election costs on an ongoing basis than ongoing election costs in optical scan counties. The two DRE counties in the study, Wake and Durham, averaged about $5.01 per voter per election when all costs were considered. The optical scan counties, Guilford and Mecklenburg, averaged $3.59 per voter.[5] In addition, an analysis of Georgia's costs showed that support, maintenance, and operation costs over a six year period were about 50% higher for DREs than for optical scan.[6]

Tennessee's largest county to use optical scan currently, Hamilton County, reports that ballot printing costs about 15 to 20 cents per ballot. The county also reports that they do not have to print excessive numbers of ballots, even for early voting, and that the

It would cost about $12 million to purchase an optical scan machine for each of the roughly 2,300 precincts that lack them and $12.5 million to purchase automatic ballot marking devices for all counties if one DRE per precinct is kept for disability access (as Hamilton and Pickett counties do now), the change could be made for approximately $12 million.

ballot-printing costs associated with their optical scan system are not prohibitive. If early voting with its attendant central voting locations does require substantial ballot printing costs, the option of "ballot on demand" exists.

Ballot on demand is a system allowing poll workers to print the proper ballot for a voter when he arrives to vote, eliminating the need for estimating the number of each type of ballot needed and overprinting to be sure enough ballots will be available. Florida, which is switching to optical scan for all of its counties, will make use of ballot on demand for early voting.

Verifiable votes and audit trails have other costs as well. Verifying the paper ballot adds a step that can slow down the voting process. Voters may become confused while trying to verify that the votes on the computer screen match those on the paper ballot. Some of the VVPAT devices currently in use produce a printout that is so compact that it is difficult to read. Both problems may discourage voters from reviewing their ballots before pressing the final 'vote' button to cast the ballot. Researchers at the Massachusetts Institute of Technology and California Institute of Technology suggest aural verification using headphones to listen to a voice recite the votes as cast. They argue that most people find this process easier to follow and understand. It also mirrors the audio systems currently in place to assist voters with visual impairments, but it does not offer a paper trail.

If too few machines are available for the voters at a precinct, lines may be long and slow. Slow lines discourage voters and can effectively restrict access to the polls by causing voters to leave before they cast their ballots. Optical scan balloting has the advantage in this regard, as each voter needs only a private booth, not an expensive piece of equipment, to complete her ballot. More voters may cast their ballots at the same time without the additional cost. But optical scan voting can also move slowly if voters fail to use the correct type of pencil or pen or if voters make too many stray marks, causing their ballots to be rejected by the scanning equipment. Replacing spoiled ballots leads to longer times to vote, security concerns in keeping up with good versus spoiled ballots, and additional time for the voter to go through the ballot again.

> If too few machines are available for the voters at a precinct, lines may be long and slow. Optical scan balloting has the advantage in this regard, as each voter needs only a private booth, not an expensive piece of equipment, to complete her ballot.

Other problems are posed by the paper itself. Adding printers to DRE machines increases the chance of equipment malfunctions, such as paper jams and ink or paper shortages. And even optical scan precincts must have either a DRE or a ballot marking device to help disabled voters cast their votes privately. These are also subject to additional equipment malfunctions.

For both types of paper record balloting, the massive amount of paper that must be handled by poll workers raises security issues. Paper can be damaged, lost, mishandled, or stolen. Furthermore, both kinds of machines are subject to hacking and software tampering to change vote totals. But even so, paper trails reassure voters that their vote is being counted accurately and can be audited or recounted.

It is possible to reduce some of these costs by taking other steps to remove some of the pressure on polling places on election day. Tennessee has one of the more robust early voting programs, with nearly half of the ballots in 2006 across the state being cast before election day. Some other states also allow more freedom to vote absentee, and a significant portion of voters do so in many states.

MAKING USE OF EXISTING HAVA FUNDS

When Florida's current Governor Charlie Crist asked the state legislature to require optical scan machines in all precincts in the state, he requested that the EAC allow him to spend some of Florida's remaining HAVA funds on the change. In a written response, Juliet T. Hodgkins, General Counsel for the EAC, stated that counties which had already used HAVA funds to replace their voting machines could not do so again.

Some counties in Florida had compliant machines already and had not replaced them, so a portion of Florida's HAVA funds were available for use. The state was also allowed to use any funds it raised by selling or trading the voting machines it was replacing. Finally, the Ballot on Demand system that Florida planned to purchase (this system allows the proper ballot to be printed for voters as they arrive at the polls, eliminating the need for pre-printing ballots) was a valid use of remaining HAVA funds.

In a 2004 pilot program in San Bernadino, a manual recount of one precinct took an average of 21 minutes per ballot. The subsequent report recommended high speed readers be used to tally the votes.

According to State Election Coordinator Brook Thompson, Tennessee has about $35 million in HAVA funds remaining, some of which is planned for use in improvements in the statewide voter database.

Using this opinion as a guide, one could conclude that Tennessee would have some HAVA funds available for use. According to State Election Coordinator Brook Thompson, Tennessee has almost $35 million in HAVA funds remaining, some of which is planned for use in improvements in the statewide voter database. Some of these funds could likely be used to purchase a Ballot on Demand system, which would alleviate the concerns about pre-printing ballots, especially for early voting.

In addition, six Tennessee counties kept their Microvote 464 systems and only used HAVA funds to purchase one DRE per precinct for disability access. A few other counties already had compliant systems when HAVA was passed. Some HAVA funds might be available for machine replacement in these counties.

EXPERIENCES WITH DRES WITH VVPAT

Nevada was the first state to implement electronic voting with voter verifiable paper records. Sequoia's AVC Edge machines with the VeriVote printers were used throughout the state for the September 2004 primary election, as well as the November 2004 general election. Neither election officials nor voters were able to physically handle the paper ballots. Instead, after each voter made his or her selections, a printout was displayed behind a glass window. The voter then either verified that the printout was correct or rejected it and started the selection process again. Once the voter verified the ballot, it was stored inside a ballot box.

The Nevada elections were viewed as a success. "Primary voters across the state cast votes on machines that printed out paper records, and none of the nightmarish possibilities came to pass."[7] But later elections showed the difficulties that can arise when recounts are needed of paper rolls attached to DREs. Figure 3 is a photo of a Clark County, Nevada election worker holding one end of a 318-foot DRE VVPAT tape. This tape contains only 64 ballots.

One month after the primary election in Nevada, the County of San Bernardino in California announced that it had been approved by the California Secretary of State to serve as a pilot program for VVPAT during the November 2004 presidential election. The

Figure 3. Photo reprinted with permission of Larry Lomax, Registrar of Voters, Clark County, Nevada

The printer attachments for DREs have some drawbacks if they are to be recounted or audited. The woman in this photo holds one end of a 318-foot DRE voting machine tape which contains only 64 ballots.

precinct where the pilot program was tested used the same system as the state of Nevada. Only 270 of the 1,495 voters in the precinct used it to cast their ballots. A joint report by the San Bernardino County Registrar of Voters and Sequoia Voting Systems characterized voters' comments about their experiences as positive; however, the manual recount that followed as part of the pilot was not.

Three teams of two staff members each worked two 8-hour days to recount every race on the ballot—adjusting for human counting errors along the way—and confirm that the totals on the paper rolls matched the electronic tally for every race. That works out to 270 ballots recounted in 96 staff hours, which equates to either 2.8 ballots per hour or just over 21 minutes per ballot. The report authors claimed that the manual recount process would be less time consuming if high-speed readers were used to help tally the votes. It also recommended that machine-specific identification be placed on the paper rolls so that totals from individual machines could be verified, as well as precinct totals. The final recommendation of the report was to grant full certification of the system.

A report of a San Bernadino, California manual recount showed that election workers averaged 21 minutes per ballot for the DRE printer attachment rolls.

Unlike the Sequoia system, not all voting systems with paper ballots have received positive recommendations. In July 2005, after finding a 10% error rate in a mock election of 96 machines, former California Secretary of State Bruce McPherson rejected Diebold's application to certify the AccuVote-TSx with AccuView Printer Module. The machines also experienced printing jams and screen freezes. During the May 2006 primary election in Cuyahoga County, Ohio, multiple failures were documented for the Diebold AccuVote-TSx with AccuView Printer Module:[8]

- paper jams,

- voter access card failures,

- electrical problems caused by a missing electrical adapter on the touch screen machines,

- lost electronic ballot boxes in two counties, and

- computer screens that did not match the ballot printout.

Cuyahoga County hired San Francisco based Election Science Institute (ESI), a non-partisan, non-profit organization, to investigate problems encountered during the May 2006 election. ESI's August 2006 report, *DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio,* included eight key findings:

1. After three months of exhaustive research, empirical evidence supports the key definitive finding: The machines' four sources of vote totals—VVPAT individual ballots, VVPAT summary, election archive, and memory cards— did not agree with one another.

2. The vast majority of voters surveyed were pleased with their experience with the new system, liked touch screen voting, and had confidence that their votes would be recorded correctly.

3. Improved training, both practical and procedural, is likely to minimize incidents experienced on election day.

4. Incident reports were numerous but concentrated, with 9% of precincts reporting 10 or more

A report on Cuyahoga County, Ohio's May 2006 primary using DREs with VVPAT found multiple problems.

incidents. The most commonly reported incidents were voter registration issues (30.1%), election administration issues (22.6%), problems related to voting machines (16.2%), and issues involving booth workers (9.1%).

5. New strategies for voting machine allocation are needed to minimize voter wait time and distribute it equally across all locations.

6. VVPATs were missing or missing information and the tally of the individual ballots did not always match the VVPAT summary printed at the end of election day.

7. Discrepancies were found across vote counts stored on different mediums across the election system.

8. The current election system, if left unchanged, contains significant threats to inventory control of mission-critical election assets, error-free vote tabulation, and tabulation transparency. One likely result is diminished public confidence in a close election.

Diebold Elections Systems, Inc. denied that any of the problems were the result of voting machines and printers. Instead, Diebold investigators argued that human error was behind the problems and that they could be corrected with more education for voters, poll workers, and election administrators.

EXPERIENCES WITH OPTICAL SCAN

While optical scanning technology offers the advantages and efficiencies of instant counting, the integrity of the results recorded by these devices still depends on election workers' ability to properly secure and monitor optical scan equipment. A 2006 report by the University of Connecticut, *Security Assessment of the Diebold Optical Scan Voting Terminal*, identified a number of vulnerabilities in the system that, if exploited maliciously, could invalidate the results of an election. The review was supported by the Connecticut Secretary of State's Office and carried out by

the Voting Technology Research Center and the university's department of computer science and engineering. The researchers found that the system could be compromised with off-the-shelf equipment—like paper clips, a standard serial cable, or a telephone cord—in a matter of minutes even with its removable memory card sealed in place, and without access to the proprietary software:

> The basic attack can be applied to effect a variety of results, including entirely neutralizing one candidate so that their votes are not counted, swapping the votes of two candidates, or biasing the results by shifting some votes from one candidate to another. **Such vote tabulation corruptions can lay dormant until the election day, thus avoiding detection through pre-election tests.** [Emphasis added.]

The report's authors note the similarity between optical scan systems and DRE voting machines in terms of these vulnerabilities but emphasize the key difference, which is that optical scan systems have a built-in, hand countable VVPAT:

> An important benefit of using the optical scan technology in electronic voting systems is that it naturally yields a voter-verified paper trail—the actual "bubble sheet" ballots marked by the voters. This differentiates optical scan electronic voting from DRE (direct recording electronic) electronic voting terminals (such as the Diebold AccuVote TS and TSx terminals) that provide a digital interface for voting during the elections. We note that the current generation of the DRE terminals—especially paperless ones—have received substantial criticism due to a number of critical security vulnerabilities . . . Even when a DRE terminal is equipped with a printer, the computer-generated paper trail cannot be directly considered voter-verified, and it is possible for a faulty DRE to print spontaneous ballots while unobserved. Further development of the DRE technology is necessary for it to become a trustworthy alternative. . . . While optical scan voting is freed from some of the perils of

The Voting Technology Resource Center report strongly advised post-election audits, a requirement adopted in a number of states and jurisdictions for a wide variety of voting systems.

paperless trails or computer generated paper trails, the election still relies on the terminal to electronically add the votes and report the results; this introduces the possibility of attacks that interfere with these basic tabulation and reporting tasks.

The authors also set out some new safe-use recommendations for the system:

- Install tamper-resistant seals for removable memory cards, serial port, telephone jacks, as well as the screws that allow access to the terminal's interior—failure to seal any single one of these components renders the terminal susceptible to attack outlined above. An alternative is to seal the entire Optical Scan system (sans ballot box) into a tamper-resistant container at all times other than preparation for election and deployment in an election.

- Enforce an unbroken chain of custody at all times.

They also advised post-election audits, a requirement adopted in a number of states for a wide variety of voting systems.

Hamilton County is one of two Tennessee counties using an optical scan voting system, and the local election commission office reports that they are very satisfied with this system and would highly recommend it to other interested counties. They report that it is reliable and that they have not had significant problems using this system. Pickett County uses a system made by ES&S that is similar to the Diebold technology. Pickett County also reports that they are pleased with their optical scan system and have not had any problems using this technology.

LEGISLATIVE ACTION IN TENNESSEE

Seven bills filed in the General Assembly during the last session require some form of paper audit trails. All were referred to their respective State and Local Government Committees, which put them in subcommittee pending a recommendation by the Joint Study Committee on the Voter Confidence Act of 2006.

Sixteen states with paper-based ballot systems or electronic voting machines with paper trails require manual post-election audits in which a portion of ballots or paper records are counted by hand and compared to the total in their precinct for consistency.

- **HB1256/SB1363** required a voter verified paper ballot to serve as the ballot of record for all new voting machines purchased after the passage of the legislation. It further required expedited updating of existing machines to come into compliance.

  This bill required VVPAT and applied to new machines with expedited replacement of existing machines. Optical scan and DRE with VVPAT would comply. The fiscal note was $9.535 million.

- **HB1282/SB0824** required that all voting systems purchased after July 1, 2007 produce a paper version of all ballots at the time they are cast and that version be retained by the county election commission for any recounts, contests, or random samplings for accuracy.

  This bill required VVPAT and applied to new machines only. Optical scan and DRE with VVPAT would comply. The fiscal note was "not significant" as the new standards apply only on a going forward basis.

- **HB1373/SB1217** required that, by the November general election to be held in 2008, each voting machine be capable of producing a hard copy of the voting totals. The machine may have a documented method in place capable of retrieving the voting totals stored in the machine and producing a hard copy of such voting totals.

  This bill codified practices already in place concerning the printing of vote totals. Optical scan and DREs (with or without VVPAT) would comply. The fiscal note was "minimal."

- **HB 1764/SB0639** required a Voter Verified Paper Audit Trail for all computerized DREs.

  This bill required VVPAT. Optical scan and DRE with VVPAT would comply. The fiscal note was $9.535 million.

- **HB1894/SB1697** required that all voting systems purchased after July 1, 2007 produce a paper version of

all ballots at the time they are cast and that version be retained by the county election commission for any recounts, contests, or random samplings for accuracy.

This bill required VVPAT and applied to new machines with expedited replacement of existing machines. Optical scan and DRE with VVPAT would comply. The fiscal note was "not significant" as the new standards apply only on a going forward basis.

- **HB1896/SB1700** required a voter verified paper ballot to serve as the ballot of record for all new voting machines purchased after the passage of the legislation. It further required expedited updating of existing machines to come into compliance.

  This bill requires VVPAT and applies to new machines with expedited replacement of existing machines. Optical scan and DRE with VVPAT would comply. The fiscal note was $9.535 million.

- **HB2152/SB2033** required that all ballots be marked by the voter (with provisions for those with disabilities), be available for voter verification, and be retained by the county election commission for any recounts, contests, or random samplings for accuracy.

  This bill required that the voter mark the ballot and applies to new machines with expedited replacement of existing machines. Though TACIR staff interpreted this bill to mean that only optical scan machines and hand-counted paper ballots would comply, the fiscal note (the same $9.535 million as the bills above) appears to have assumed that DREs with VVPAT would also comply.

EARLY VOTING, ABSENTEE VOTING, AND VOTE BY MAIL

One of the concerns with voter verified paper audit trails is the extra time it will take voters to complete the voting process. This can mean longer lines, decreased poll access, and extra expenditures for more voting machines. One of the best ways to deal with these expenses is to take some of the pressure off of polling places on election day through the use of early voting and voting by mail (no excuse absentee voting).

Tennessee is one of 31 states that allows no-excuse early voting or in-person absentee voting. Only five of those 31, including Tennessee, require an excuse to vote absentee by mail.[9]

EARLY VOTING EXPERIENCES

Research on this issue does not separate early, in-person voting from early voting that includes no-excuse absentee voting by mail. The five states that allow no-excuse early voting but not no-excuse absentee voting by mail are Indiana, Nevada, Tennessee, Texas, and West Virginia. The latest research on the combined types of early voting shows a small increase in turnout in mid-terms and smaller elections by encouraging voters who normally vote only in larger elections to participate.[10]

According to the Division of Elections' website, more than half of voters in several Tennessee counties voted early in 2006. The early vote percentage for the state as a whole was 45.5% and 1.8% cast their ballot absentee by mail. Based on these statistics, early voting is quite popular in Tennessee. But the opportunity to vote early is not the same for everyone in the state. Legislators have heard complaints from voters outside of cities that early voting is not available to them or is available for such a brief time or with such long waits that it is difficult to take advantage of the opportunity.

A study of the Florida early voting experience in 2004 found similar complaints: the demand for early voting was underestimated (in the first early voting election in Florida, 30% of the vote was cast before election day) and sites were too few and overcrowded.

Several counties in Tennessee had more than half of their voters who turned out for the election vote early in 2006, while the state as a whole saw an early vote percentage of 45.51% and an absentee vote by mail percentage of 1.84%.

The study notes that Georgia and North Carolina made the same mistake.[11] Studies of national election reforms show that early voting and relaxed absentee voting regulations are popular with voters, and their use is still increasing annually.[12]

ABSENTEE VOTING

Absentee voting by mail in Tennessee is available only to those over 65 years of age (as it may be more difficult to get to the polls- four other states have such exemptions), in the military, or unable to make it to the polls during regular voting times. Tennessee is one of 22 states with such restrictions on absentee voting by mail. Some states have come to rely quite heavily on the practice, including Oregon, where voting by mail is the only option. Those states have found that allowing widespread absentee voting by mail increases turnout and saves money.

THE OREGON EXPERIENCE–VOTING SOLELY BY MAIL

Attitudes toward Oregon's all vote-by-mail method appear to be generally positive in that state. A 2003 survey by the University of Oregon found that: "the overwhelming support for vote-by-mail is apparent (80.9%), and this preference is consistent across all demographic and attitudinal subcategories." Multnomah County (Portland), Oregon, posts the following information on its web site:

> In 1998 voters passed a ballot measure directing all elections to be conducted by mail, commonly called Vote By Mail. Instead of using traditional polling places where voters go to cast ballots on election day, a ballot is mailed to each registered voter. The ballot is then returned to the county elections office and is counted on election day.

Election Preview 2006, published by electionline.org, states that, "Oregon is also in the process of deploying a new vote-by-phone system accessible to voters with disabilities at county election offices." In the November 2006 general election, all of Oregon's 36 counties "provide[d] an accessible ballot marking station at each county election office using a telephone and fax machine to

A 2003 survey by the University of Oregon found that 80.9% of Oregon voters support vote-by-mail, and this preference is consistent across all demographic and attitudinal subcategories.

afford voters with disabilities the opportunity to vote privately and independently."

Oregon's Secretary of State, Bill Bradbury, is upbeat about his state's all vote-by-mail elections. After the 2004 presidential election, he wrote a commentary titled "Vote-by-Mail: The Real Winner Is Democracy" that appeared in the January 1, 2005, edition of the *Washington Post*. In it, he described the presidential election of 2004 as one "with record turnout and little strife." He claims it is "reliable and popular," and that "signature verification of every voter before a ballot is counted is an effective safeguard against fraud." As for financial savings, he says, "the cost of a vote-by-mail election is nearly 30 percent less than the cost of a polling place election." And about turnout he said, "record numbers of Oregonians registered to vote, and almost 87% of them [registered voters] cast ballots." Finally, he pointed out that the untraditional method of voting at home allows for children to see the actual ballot and brings them closer to the election process.

OTHER STATES' EXPERIENCES

In addition to Oregon, two other west coast states were found to use vote-by-mail extensively in their elections:

- Washington: "Currently, 34 of Washington's 39 counties vote entirely by mail. Of the five counties that maintain poll sites, 61.31% of the votes were cast by absentee ballot in the 2004 General Election … Absentee ballots must be signed and postmarked or delivered to the county election officer on or before election day."[13]

- California: "During California's latest election in November [2006], nearly 42% of voters turned in absentee ballots— continuing the mailbox trend. Of the state's 58 counties, 16 received more absentee ballots than votes cast directly at polling places. Given the convenience, many election officials say it's no surprise that absentee ballots have become so popular … But voter advocates have mixed feelings, noting that California has 58 different voting systems, compared with one in Oregon."[14]

Thirty-four of Washington's 39 counties vote entirely by mail. In the remaining five counties, 61.31% of voters voted absentee.

During California's latest election, nearly 42% of voters turned in absentee ballots.

UNIQUE CONCERNS ABOUT FRAUD

Though some areas count mailed ballots by hand, many use optical scan ballots for voting by mail. Depending on how the ballots are counted, voting by mail can involve many of the same problems encountered with electronic vote tally machines used at the polls. As it is possible for voters to fill out their ballots in front of others or in groups, votes cast by mail can be more easily bartered, sold, or coerced.* Those opposed to "no excuse" voting by mail claim the system is inherently conducive to fraud. Proponents and those currently using it claim that such incidents have not occurred in practice.

LEGISLATIVE ACTION IN TENNESSEE

Four bills related to early voting, vote by mail, and absentee voting (generally grouped with early and by mail voting) were filed in the General Assembly in the last session. Two of these bills were referred to the Joint Study Committee on the Voter Confidence Act of 2006.

- **HB0016/SB0018** proposed extending early voting by one week.

  The fiscal note was $1.526 million twice every two years. This bill was withdrawn.

- **HB0017/SB0012** would have allowed any voter to vote absentee without showing cause.

  This bill allowed "no excuse" absentee balloting. This bill was recommended by the Joint Study Committee on the Voter Confidence Act of 2006 and was in subcommittee in both the House and Senate State and Local Government Committees. The fiscal note was $305,000 one time and $1,930,000 twice every two years. Future amounts assumed 15% to 25% of voters will vote absentee eventually and included those costs. It did not include savings from

---

*Voters may also take someone into the voting booth with them at the polls, but, if the same person accompanied several voters, suspicions would be raised in a way that they would not if the same situation occurred away from the polls.

those voters not going to the polls as they could not be quantified.

- **HB0485/SB0642** required elections to be conducted by mail.

  This bill was sent to the Joint Study Committee on the Voter Confidence Act of 2006, which directed its Senate sponsor, Senator Beverly Marrero, to work with State Election Coordinator Brook Thompson to identify counties that wish to participate in a Vote by Mail pilot program. The bill was referred to the State and Local Government Committees of both Houses; the Senate placed it in subcommittee.

- **HB1916/SB0923** clarified that the names of those making absentee ballot requests are not to be released before the end of early voting.

  This bill became Public Chapter 152.

FEDERAL RESEARCH AND INITIATIVES

Tennessee should not evaluate voting machinery in a vacuum. This issue is also being addressed at the federal level; both through research by the EAC and through legislation introduced this session in the United States Congress. While Tennessee should seek to coordinate whatever recommendations it makes with federal findings and potential new federal laws, waiting for Congressional action may not be advisable.

THE EAC AND VVPAT RESEARCH

The EAC was established in 2002 by HAVA. It is meant to be a national clearinghouse and resource for federal elections information and procedures. HAVA required the EAC to

- generate technical guidance on the administration of federal elections;

- produce voluntary voting systems guidelines;

- research and report on matters that affect the administration of federal elections;

- otherwise provide information and guidance with respect to laws, procedures, and technologies affecting the administration of Federal elections;

- administer payments to states to meet HAVA requirements;

- provide grants for election technology development and for pilot programs to test election technology;

- manage funds targeted to certain programs designed to encourage youth participation in elections;

- develop a national program for the testing, certification, and decertification of voting systems;

- maintain the national mail voter registration form that was developed in accordance with the National Voter Registration Act of 1993 (NVRA), report to Congress every two years on the impact of the NVRA on the administration

Election issues are also being addressed at the federal level; both through research by the U.S. Election Assistance Commission (EAC) and through legislation introduced this session in the United States Congress.

of federal elections, and provide information to States on their responsibilities under that law;

- audit bodies who received federal funds authorized by HAVA from the General Services Administration or the EAC; and

- submit an annual report to Congress describing EAC activities for the previous fiscal year.

The EAC has produced a Best Practices Tool Kit for election administration, including solutions, examples, and suggested resources for voting systems in general and specifically for each type of system.

Toward its mission, the EAC has produced a Best Practices Tool Kit for election administration. The kit includes solutions, examples, and suggested resources for voting systems in general and specifically for each type of system, including DRE systems. The tool kit includes recommendations for security and management of systems prior to, the day of, and after election day. Neither the recommendations for DRE systems nor those for any of the other systems specifically include the use of voter verified paper audit trails. The EAC's election day and post-election recommendations include the following:

- Election day

    o Control access to the voter "smart cards." Educate poll workers and voters to know that the "smart card" is not the ballot and the voter's choices are not recorded on the "smart card." The card merely directs the voting unit to bring forward the voter's correct voting screens.

    o Develop a plan to provide election day technical support for poll workers, including a troubleshooting checklist, a call center, and roving technical personnel.

    o Establish written procedures for handling election day equipment failure.

    o Provide for redundant records of results, including paper printouts.

    o Ensure transparency in all aspects of the tabulation process, especially in the transport or transmission of results to the central election office.

o   Develop chain of custody for memory cards and machines.

- Post-Election

    o   Conduct post-election logic and accuracy testing of machines.

    o   Modem unofficial results over phone line using encryption to protect data during transmission.

    o   Conduct a post-election audit to reconcile all records, especially the number of voters and the number of votes cast.

    o   Conduct a public post-election "debriefing" to address any concerns related to the voting system.

A preliminary staff review of the EAC research did not identify any endorsement for VVPAT; however, a search of the EAC website did locate a useful resource on the topic. That resource, *Security Vulnerabilities and Problems with VVPT*, an April 2004 paper by Ted Selker and Jon Goler, reminds us that some forms of VVPAT are not without their own security concerns. Selker and Goler note that VVPAT additions to DREs have the following problems:

- ergonomic problems that could be introduced by the receipt having a different layout than the ballot, by voters having difficulty remembering previous selections to make the verification, by requiring an extra step after making selections, and by VVPT being difficult to use by sightless people;

- logistics problems that include difficulties in collecting and organizing the receipts, transporting them, and reading and reconciling them with electronic tallies;

- security issues that include possible misprinting of receipts in a manner that cannot be detected and that hand counting does not easily detect fraud; and

- mechanical problems that include printer breakdowns and running out of supplies.

VVPAT printouts have a different format than the ballot on the screen, and they may be reviewed after completing a long ballot with many choices to remember. There have been no real world or experimental demonstrations yet that prove that voters can successfully verify their ballots using a paper receipt.

Two bills in the U.S. Congress are currently under consideration that would require paper trails. The "Holt Bill" originated in the U.S. House of Representatives, sponsored by Representative Rush Holt (D-NJ) and the "Feinstein Bill" originated in the U.S. Senate sponsored by Senator Diane Feinstein (D-CA).

Selker and Goler also note that there have been no real world or experimental demonstrations yet that prove that voters can successfully verify their ballots using a paper receipt. They suggest consideration of possible alternatives to VVPAT, including votemeters (an external device from a different manufacturer that tallies votes for comparison) and voter verified audio transcripts (an audio read back of voter selections for verification).

Nonetheless, in a sign that the move toward auditable paper records has reached a tipping point, the EAC is completely revamping its "voluntary guidelines" for states for choosing voting machines. These guidelines are voluntary because states do not have to choose federally-certified voting machines, but only machines that meet the guidelines will be federally certified.

The EAC issued a press release on September 6, 2007 announcing that it had received a 598-page draft report from its Technical Guidelines Development Committee recommending that future guidelines

- allow auditing of voting system records independently from the voting system's software,

- allow each voter to verify the accuracy of their vote before leaving the polling station,

- improve voting system reliability and reduce problems with failing machines on election day,

- tighten security measures through digital signatures and other means to protect voting system software against unauthorized alterations, and

- ensure voting systems are relatively easy to use accurately based on the results of laboratory tests in which participants vote in mock elections.

The EAC must take public comments, make revisions based on those comments, and then take public comments again, so its new guidelines are not expected to take effect until January 2009, and they may differ somewhat from the Technical Guidelines Development Committee's recommendations.

FEDERAL LEGISLATIVE ACTION

Two bills in the U.S. Congress are currently under consideration that would require paper trails, the "Voter Confidence and Increased Accessibility Act of 2007" (also known as the "Holt bill") and the "Ballot Integrity Act of 2007" (also known as the "Feinstein bill"). There are two additional bills, the "Count Every Vote Act of 2007" has thin support in the House, and most of its Senate sponsors have also sponsored the Feinstein bill, which has much more momentum, though it lacks a House companion bill. The "Verifying the Outcome of Tomorrow's Elections Act of 2007" has only one House cosponsor and no Senate companion bill.

The Holt bill (HR 811), introduced by Representative Rush D. Holt of New Jersey, would require that the voting system use or produce an individual voter-verified paper ballot of the voter's vote that shall be created by or made available for inspection and verification by the voter before the voter's vote is cast and counted.

The paper ballot can be produced by various methods–-hand marking, optical scan, DRE, or other machines—as long as the voter is allowed to verify the ballot in paper format. The paper record would be the ballot of record for all recounts and audits. Paper ballots would be on archival quality paper and would be maintained for audit purposes, but not in a manner that would allow the confidentiality of an individual's vote to be compromised. As currently written, the bill would require that ballots be separated as they are printed. This requirement, along with the paper quality requirement, would exclude existing DRE printer add-on technology.

The bill requires that election source code be made publicly available. In addition, audits would be required before certifying election results, with the number of ballots to be hand-counted tied to the total number of precincts and the closeness of the race. The federal government would reimburse the states for "reasonable" costs associated with implementation of the Act. To date, H.R. 811 has acquired 216 co-sponsors, including Representatives Cohen, Cooper, Davis, Gordon, Tanner, and Wamp of Tennessee. This Senate companion bill is S. 559,

As currently written, both the "Holt Bill" and the "Feinstein Bill" would exclude existing DRE printer add-on techonolgy.

The passage of either of the two bills under serious consideration as currently written would require replacement of Tennessee's DRE's, though there has been movement to amend the "Feinstein Bill" to allow DRE vendors more time to develop a printer attachment for their machines that would comply.

sponsored by Senator Bill Nelson (D-FL). It currently has no cosponsors.

The Feinstein bill has very similar language requiring a voter verified paper record, though the paper version is a "record" and not the official ballot as it is in the Holt bill. The Feinstein bill gives states until 2010 to meet its standards, a move which is increasingly seen as necessary as the 2008 elections rapidly approach. There are many other differences, as both bills have many sections, but these are the key differences in their paper record requirements. The Feinstein bill does not currently have a House companion bill.

The "Count Every Vote Act of 2007" was sponsored by Representative Stephanie Tubbs Jones (D-OH) and Senator Hillary Rodham Clinton (D-NY). It has 19 cosponsors in the House and 7 high-profile cosponsors in the Senate, but most of its Senate supporters (including sponsor Clinton) have since cosponsored the Feinstein bill.

The Jones/Clinton bill stands out in that it has extensive grant programs for pilot projects in states to encourage activities such as civic education in high school and same-day voter registration. It also requires and funds federal research into many aspects of elections, including ballot design, ballot chain of custody, and disability access. Finally, it would fund all of its requirements, including voting machine updates and ongoing post-election audits. This bill, however, currently has no traction in Congress.

The other bill introduced this session, the Verifying the Outcome of Tomorrow's Elections Act of 2007 (HR 879), introduced by Representative Tom Feeney (R-FL), is primarily a bill requiring voters to provide photograph identification in order to vote (even by mail), but the Act does also include a requirement for a paper receipt. It also shows no movement in the House and has no Senate companion bill.

The passage of either of the two bills under serious consideration as currently written would require replacement of Tennessee's DREs, though there has been movement to amend the "Feinstein

Bill″ to allow DRE vendors more time to develop a printer attachment for their machines that would comply.

In addition to these VVPAT bills, two bills have been introduced to address vote by mail. The first, H. R. 1667 by Representative Susan Davis (D-CA) and S. 979 by Senator Ron Wyden (D-OR), would help fund the switch to vote by mail as long as it followed Oregon's standards. Funding could be obtained to switch whole states, groups of counties, or individual counties to the program. Eighteen million dollars would be available as the bill is currently written. The Senate bill has been cosponsored by Senator John Kerry (D-MA) and Senator Barack Obama (D-IL). The House bill has 4 cosponsors.

The second vote by mail bill that has been introduced in the House this session would require states to allow voters who so wished to vote by mail. Representative Susan A. Davis of California introduced the bill, the Universal Right to Vote by Mail Act of 2007 (H.R. 281). H.R. 281 would require that

> (if) an individual in a State is eligible to cast a vote in an election for Federal office, the State may not impose any additional conditions or requirements on the eligibility of the individual to cast the vote in such election by mail, except to the extent that the State imposes a deadline for requesting the ballot and related voting materials from the appropriate State or local election official and for returning the ballot to the appropriate State or local election official.

H.R. 281 does not appear to address reimbursing states for any associated implementation costs. The bill, which has 62 co-sponsors, was referred to the House Committee on House Administration on January 5, 2007. There is no Senate companion bill as yet.

Each of these four bills would be effective beginning with the federal elections of 2008. The passage of any of the four would undoubtedly impact Tennessee's ability to address its own concerns with voter access and security.

VERIFYING THE SOFTWARE–SOURCE CODE AND TRADE SECRETS

Headlines over the last several years have brought the arcane language of computer scientists and intellectual property lawyers into common parlance. Among the concerns about voting machines is the inability to review the software or programs that store and tally the votes. The software is called "source code," and the main impediment to its disclosure is state "trade secrets" law. Source code is a sequence of instructions written by a computer programmer in a high-level language like FORTRAN or COBOL that is readable by people but not by computers. Source code must be converted into object code by a compiler or interpreter in order to be executed by a computer. Source code is proprietary information that is protected by copyright law and trade secrets law.[15]

COPYRIGHT LAW AND TRADE SECRETS LAW

Copyright law protects against the unauthorized copying of proprietary information, so analyzing source codes would not violate copyright law. Trade secrets are information such as a formula, pattern, compilation, program, device, method, technique, or process that derives economic value from not being generally known and is subject to reasonable efforts to preserve confidentiality. Businesses use trade secrets to secure advantage over others in the same industry. Trade secret law prevents others from misappropriating and using the trade secret. It may prevent access to voting machines' software source codes.

Trade secret law is generally adjudicated at the state level, though federal preemption of state laws would be possible.

PLACING SOURCE CODE IN ESCROW

As a part of its software licensing agreements, a vendor will often place its software source code with a third-party escrow agent so that the person or business holding the license will still have access to it if the vendor goes out of business. The escrow agent simply holds the software for the parties to the license but cannot read or access it. A number of companies specialize in software escrow.

> Analyzing source codes would not violate copyright law, but trade secret law may prevent access to voting machine software source codes. Trade secret law is generally adjudicated at the state level, though federal preemption of state law would be possible.

The Commission on Federal Election Reform endorsed this technique for voting machine software in its final report issued in September 2005, *Building Confidence in U.S. Elections*:

> Manufacturers of voting machines have legitimate reason to keep their voting machine software and its source code proprietary. The public interest in transparency and the proprietary interests of manufacturers can be reconciled by placing the source code in escrow with the National Institute of Standards and Technology (NIST), and by making the source code available for inspection on a restricted basis to qualified individuals. NIST might make the source code available to recognized computer security experts at accredited universities and to experts acting on behalf of candidates or political parties under a nondisclosure agreement, which could bar them from making information about the source code public, though they could disclose security flaws or vulnerabilities in the voting system software.[16]

THIRD-PARTY SOFTWARE

Many voting machines make use of software from other companies, primarily Microsoft. With Windows-based programming, voting machine vendors are not able to make source code public without the permission of Microsoft. And Microsoft has made clear that such permission will never come. If source code is to be made public, vendors will have to completely revamp their software so that it is based on open-source operating systems such as Linux. Experts suggest that such a move is feasible if adequate time is given to achieve it.[17]

SOURCE CODE ISSUES IN OTHER STATES

Eleven states currently require DRE voting machine vendors to place their source code in escrow:

California	Michigan	South Carolina
Colorado	North Carolina	Wisconsin
Illinois	Ohio	
Indiana	Oklahoma	

Eleven states currently require DRE voting machine vendors to place their source code in escrow (file it with a third party so the state may later access it if necessary).

According to Matt Zimmerman, attorney for the Electronic Frontier Foundation (EFF), most of these state laws were passed to ensure that the states will have access to the source codes if the vendors go out of business.[18]

In a recent Florida case, Congressional candidate Christine Jennings and a group of voter advocacy groups filed suit to gain access to the electronic voting machine software source codes after 18,000 ballots cast on the machines registered no vote in the 13th District race in Sarasota County. The plaintiffs wanted an independent review of source codes in order to determine whether there was a system malfunction.

Trade secret law is enacted at the state level, and it governs most questions about whether or not companies can be required to place source code in escrow.

The vendor, ES&S, successfully argued that its source code was protected by trade secret law and prevented the plaintiffs from gaining access to it. This is the first case of its kind.[19] All trade secret law is enacted at the state level, so this case would not directly affect other states, however, vendors may make similar arguments in cases in other states to prevent the release of source code.

North Carolina passed its Public Confidence in Elections Act in 2005. The Act decertified all existing voting equipment and instituted new requirements that must be met before election equipment can be certified by the State Board of Elections. It includes two requirements:

- all voting system software "that is relevant to functionality, setup, configuration, and operation of the voting system" must be escrowed;

- the State Board of Elections must review or designate an independent expert to review all source code made available by the vendor.

The state agreed to use HAVA allocations to cover the costs of switching voting technology for any county using equipment that was not recertified. After the passage of this act, Diebold sought certification of its equipment in North Carolina. Diebold claimed it could not escrow its full source code because it relied extensively on third party software for critical system functions. North Carolina

certified Diebold along with Sequoia Voting Systems and Election Systems and Software (ES&S) without reviewing all the systems' relevant source codes.

On behalf of North Carolina voting rights advocate Joyce McCloy, EFF filed suit against the North Carolina Board of Elections arguing that the Board had violated its obligations to perform security tests of all the systems' codes prior to certification. EFF asked the court to void the illegal certification of all three electronic voting machines and requested a temporary restraining order to prevent North Carolina counties from purchasing any of the systems until the board reviewed and certified the systems' codes.

North Carolina noted that the source code evaluation reports of the voting systems conducted by Independent Testing Authorities had been reviewed before the systems were certified by the board. North Carolina argued that although the statute refers to a mandatory pre-certification review of all source code, third party software should be exempted from this process. All the voting systems submitted to the board used third-party code to some extent. The board required vendor code to be escrowed with a pre-determined escrow agent. It required third-party code to be escrowed with the third-party code manufacturer's escrow agent. The court determined that the Board of Elections had conducted a proper review of the equipment under "a reasonable reading" of the state law. Sequoia and Diebold decided not to sell their voting equipment in North Carolina leaving only one vendor eligible to sell voting equipment in the state, ES&S.

LEGISLATIVE ACTION IN TENNESSEE

Three bills were introduced in the Tennessee General Assembly in the last session that would affect the protected status of voting machine source code. All three bills were referred to the State and Local Government Committees of the two Houses, which referred them to subcommittees pending recommendations by the Joint Study Committee on the Voter Confidence Act of 2006.

- **HB 1281/SB 825** required county election commissions to place a copy of the voting machine software in escrow before an election.

Though the North Carolina Board of Elections prevailed in a lawsuit concerning how much of vendor source code had to be placed in escrow in accordance with North Carolina law, Sequoia and Diebold decided not to sell their voting equipment in that state.

Such source code shall be used only for the purpose of recanvassing a vote, an official recount, court order or for accuracy tests required by the Secretary of State. The fiscal note was "not significant."

- **HB 1889/SB 1692** required county election commissions to place a copy of the voting machine software in escrow before an election.

Such source code shall be used only for the purpose of recanvassing a vote, an official recount, court order or for accuracy tests required by the Secretary of State. The fiscal note was "not significant."

- **HB 1895/SB 1702** allowed any person who possesses the technical expertise with respect to computer software to be given read-only access to inspect the current hardware platform and software application interface that a voter would utilize to verify its integrity. Each such computer expert must prove to the satisfaction of the registrar that such person possesses the necessary technical expertise.

The fiscal note on this bill was $621,000 two times every two years, but it refers to other portions of the bill. There was no expense recorded for this requirement.

AUDITING ELECTION RESULTS

Few who advocate paper trails believe that all elections should be recounted. Most recounts are reserved for elections that are very close or that had noted irregularities. In Tennessee, even in a close election, recounts must be requested. In contrast, several states have automatic recounts when the vote is close, and many have audits comprised of partial recounts of randomly-selected ballots or full recounts of randomly-selected precincts as a check against machine counts. Tennessee performs the latter type of audits only in response to specific complaints. In addition, at least one state (Maryland) requires audits of election procedures and practices.

AUTOMATIC RECOUNTS AND RECOUNTS UPON REQUEST

The National Conference of State Legislatures reports that, as of September 2004, 18 states required automatic recounts in close elections and 40 states allowed such recounts upon request of the losing candidate. In a few states, the losing candidate can request a recount only if the election is close (defined by the state, generally if the top two vote recipients have totals within 1% or 0.5% of one another). In five states, a party officer can request a recount, and in several states, a group of voters can petition for a recount.

Ohio is one state that requires automatic recounts if the election is close, and it allows a losing candidate to request a recount. The 2004 Presidential election results were partially recounted there (a percentage of the votes were recounted to compare to each county's total for accuracy) at the request of Green Party candidate David Cobb and Libertarian Party candidate Michael Badnarik. In Cuyahoga County (a large part of Cleveland), two election officials were recently convicted of rigging that recount by failing to choose the ballots to be recounted at random.[20]

Eighteen states have automatic recount laws:

Alabama	Maine	Oregon
Alaska	Michigan	South Carolina
Arizona	Minnesota	South Dakota
Colorado	Nebraska	Texas
Connecticut	North Dakota	Washington
Florida	Ohio	Wyoming

The National Conference of State Legislatures reports that, as of September 2004, 18 states required automatic recounts in close elections and 40 states allowed such recounts upon request of the losing candidate.

HAND BALLOT COUNT AND ELECTION RECORD AUDITS

A recent issue brief by the Election Reform Information Project at the University of Richmond[21] reports that 16 states require a hand recount of some portion of the ballots prior to certification:

Alaska	Illinois	North Carolina
Arizona	Kentucky	Utah
California	Minnesota	West Virginia
Colorado	Missouri	Wisconsin
Connecticut	New Mexico	
Hawaii	New York	

Five additional states (Florida, Nevada, Pennsylvania, Texas, and Washington) have either mandatory hand and/or mechanical recounts or non-mandatory hand recounts. Maryland requires audits of election records, and Oregon has non-mandatory audits of voting systems.

TACIR staff intends to give this issue thorough study in a later phase of this project, and will compare different types of audits and the contributions each can make toward voter confidence. This portion of the study does suggest, however, that such audits are an important part of transparent elections and results that voters will trust.

LEGISLATIVE ACTION IN TENNESSEE

- **HB1895/SB1702** codified the current practice of conducting post-election audits when a complaint is filed or when one is otherwise deemed necessary by the state election commission.

  This bill was referred to the State and Local Government Committees of the two Houses, which referred it to subcommittees pending recommendations by the Joint Study Committee on the Voter Confidence Act of 2006. The fiscal note on this bill was $621,000 two times every two years, but referred to other portions of the bill. There was no expense recorded for this requirement.

Post-election audits are an important part of conducting transparent elections.

TESTING AND AUDITING OF VOTING EQUIPMENT IN TENNESSEE

Rules governing all aspects of election procedures are in Chapter 1360-2 of Tennessee Rules and Regulations. Tennessee has separate rules for electronic, optical scan vote counting systems, and for other types of electronic voting machines. The rules governing optical scan voting systems date back to 1986; the rules for other types of electronic voting machines were adopted the following year. Both were last revised in January 1999.[22] While neither these rules nor any other provision of state law require an audit of the results of any election, they do require that the machines, or at least a sample of them, be tested prior to their use.

OPTICAL SCAN VOTING SYSTEMS

Tennessee requires each optical scan device to be tested and sealed before each election. The rules governing the tests, quoted below, involve use of both properly and improperly marked ballots. The test must be open to the public and held no later than two days before the election. Notice of the testing must be posted at least five days earlier. The ballots and the results must be sealed and held by the election officials, and the vote counter must be reset to zero.

1. A series of properly marked test ballots from the manufacturer or an independent auditing firm of CPAs shall be inserted in each vote counter to insure that the vote counter will accurately count votes for each candidate and each proposition or measure.

2. A series of improperly marked test ballots shall also be inserted into the vote counter to ensure that votes will not be counted contrary to the program and election requirements.

3. The testing shall be open to the public and held no later than 2 days before the election. At least 5 days prior to testing, the presiding officer of the authority holding the election shall cause to be

Tennessee requires each optical scan device to be tested and sealed before each election.

In Tennessee, the rules governing testing of DRE voting machines are fairly specific, but are far less specific than those for optical scan systems, requiring that only 1% of the machines be tested before each election. Moreover, the requirement as written appears to apply only to the form and not the results of the vote.

published in the public press and posted in the county courthouse or other public location(s) the date, time, and place the testing will be conducted. The candidates or their representatives, as well as representatives of the news media and, in partisan elections, representatives of the political parties, shall be permitted to observe all testing procedures.

4. The test ballots shall be either a special color or voided official ballots and be printed in sufficient quantity for this testing procedure.

5. The test ballots and the results of the testing shall be sealed and retained by the county election commission.

6. The automatic vote counter to be used as precinct counter, which is delivered to a precinct or polling place, shall be reset so that its totals are zero at the opening of the polls. The automatic vote counter shall then be sealed or locked for delivery to the precinct.

7. The automatic vote counter to be used in a central location as the central counter for absentee ballots, it shall be reset so that its totals are zero at the beginning of counting.

The ballots themselves are marked by individual voters and, obviously, can be read by humans as well as by computers, so they lend themselves more readily to auditing and recounting than more modern computerized voting systems that record, store, and tally all information electronically and produce only final vote totals.

DIRECT RECORDING ELECTRONIC (DRE) MACHINES

Interestingly, state law refers to DRE systems as "non-standard." Tennessee Code Annotated, Section 2-9-110, authorizes their use. Rules governing certification of these machines are fairly specific, covering even the ethical conduct of the vendors. The rules governing testing of DRE voting machines, however, are far less

specific than those for optical scan systems, and they require that only 1% of the machines be tested before each election. Moreover, the requirement as written, quoted below, appears to apply only to the form and not the results of the vote.

> Each county election commission using electronic voting machines shall select a number of precincts equal to at least one percent (1%) of the number of precincts in the election and have all machines used in such precincts prepared for a test election. A test election shall then be conducted on each machine to assure that all office titles and candidate names are accurately printed, positioned and functioning properly.

Some Tennessee counties had to rely on their vendors to do the mandated pre-testing for the 2006 elections because the systems were brand new, and county staff had not become sufficiently familiar with the systems to test them.

In addition to the rule governing testing, there is a rule requiring retention of results in the machines for a minimum period that might allow for a post-test or audit:

> Under the provisions of T.C.A. §2-9-108, the election results shall be retained in all machines used in the election and the memory cartridge from each such machine shall remain sealed for ten (10) days after the election, or as much longer as may be necessary because of election contest.

Some Tennessee counties had to rely on their vendors to do the mandated pre-testing for the 2006 elections because the systems were brand new and county staff had not become sufficiently familiar with the systems to test them.

VOTING MACHINE SECURITY

Tennessee's rules governing security of election equipment and ballots focus mainly on the process of sealing and unsealing or locking and unlocking them. Some chapters of the rules are more specific than others, and in some places, they are not clear about the number of people who must be present when seals are applied or altered or when machines or boxes are locked or unlocked. Having at least two people—two people who are acting independently of each other—present during these activities may be the best insurance we have against tampering. Where the rules are not now specific in that respect, it may be advisable to change them.

Even with proper seals and more than one person observing and transporting equipment and other voting materials, it may be possible to tamper with the electronic information that is loaded into them. A VVPAT would seem to discourage tampering if the election itself were subject to testing. Malicious code that runs when certain conditions are met, sometimes called a "logic bomb," can be embedded in computer programs and has caused problems for several private sector companies. It is similar to the viruses and "worms" that travel via email. A VVPAT would make it possible to detect problems such as this after votes have been tallied.

Some states and localities have included very specific "chain of custody" provisions in their election rules. These are designed to document the dates, times, and individuals who possessed or accessed voting equipment, documents, and files. Others have gone further and implemented election day tests designed to detect errors and malicious code. One such jurisdiction is Travis County, Texas. Beginning with the 2004 elections, Travis County implemented a process that involves parallel testing of a sample of machines actually delivered to polling places on election day. The process involves casting a list of pre-determined votes intermittently during the day while the polls are open and making sure the machines produce the correct total. If a "logic bomb" were present, the totals produced would be incorrect and could indicate the need for a recount.

Some states and localities have implemented election day tests designed to detect errors and malicious code.

PROCEDURES IN TENNESSEE

A limited, informal survey of county election officials suggests that local processes may vary somewhat depending on county size, resources, and perception of risk. The four most populous counties (Shelby, Davidson, Knox, and Hamilton) store their voting machines in a warehouse. The greater the number of machines a county has the greater the likelihood the machines are stored at an offsite facility. The larger counties with more machines generally have a third party deliver the machines to the designated polling sites. Most of the smaller counties may keep the machines in the county election commission office. Smaller counties may allow the precinct official to come check out the machines and return them when the election is over. Others have designated technicians that deliver the machines. Local officials advise us that the machines are always sealed prior to leaving the storage facility. We have no reason based on our inquiries to believe that they are not following the state rules governing security for the election process.

POTENTIAL STANDARDS

The EAC has produced a document that provides the basic guidelines for securing voting systems. The guidelines for physical security are broad but somewhat vague leaving much to the states and localities:

- engage county and municipal information technology staff and/or local community college or technical school staff to help conduct a security review and establish and implement applicable election management system security measures;

- create or update appropriate procedures to ensure that absentee and emergency ballot blank paper stocks are controlled at all times;

- develop physical security procedures and safeguards to document the controlled physical access to voting systems and the facility where the systems are stored. Document all security-related repairs and modifications to the physical components of the facility where voting systems are stored;

> The greater the number of machines a county has the greater the likelihood the machines are stored at an offsite facility. Most of the smaller counties may keep the machines locked up in the county election commission office.

Colorado may have the most stringent state-level security procedures, ranging from extensive training for election staff at all levels to strict environmental and security controls for storage and voting areas.

- review election office work areas to ensure that office space is appropriately isolated and that undetected access by unauthorized individuals is not possible. Review voting equipment storage and work areas to ensure that only authorized personnel have access to them;

- maintain a list of personnel who have keys to election office work areas and voting equipment storage to ensure that all keys are accounted for and only authorized personnel have keys. Develop procedures and policies requiring that keys or combination locks be changed for each election cycle;

- develop chain-of-custody procedures, use tamper-evident seals, and implement inventory control/asset management processes to ensure that voting units and associated equipment are properly and securely controlled and accounted for at all times through the election administration process;

- review all election audit trail checklists to ensure that they incorporate two-person integrity security measures, such as dual signoff.

Colorado may have the most stringent state-level security procedures, ranging from extensive training for election staff at all levels to strict environmental and security controls for storage and voting areas. For example, there are separate temperature and humidity control requirements for servers and workstations, DREs, optical scanners, VVPAT records, paper ballots, and video data records. The requirements for equipment apply year round; those for VVPAT records, paper ballots, and video data records apply for a period of 25 months.

Colorado also requires video surveillance of all areas in which election software is used for the period beginning 90 days before an election and ending 30 days after an election. Activities covered by this requirement include programming and loading memory cards, as well as tallying and reporting results. And in counties with more than 50,000 registered voters, all areas used for processing absentee ballots, including any areas used for signature verification, tabulation, or storage of voted ballots or voting equipment, must be continuously recorded on video.

POTENTIAL IMPROVEMENTS FOR TENNESSEE ELECTIONS

After reviewing what is known about voting machines, as well as practices in Tennessee and other states, TACIR staff suggests the following possible changes:

- **Implement voter-verified paper audit trails statewide within a reasonable time frame.** Distrust of voting systems that are entirely electronic is widespread, undermines voter confidence, and may discourage voting. The current system allows no check of the electronically-generated count other than one that uses the same machines and software to recount the same electronically recorded votes. Though recounts of DRE totals sometimes uncover votes that went uncounted for various reasons, they do not include a count that is independent of the voting machines. If something unusual happens in the election, especially if it involves some kind of equipment malfunction, voters are simply unsatisfied if there are no physical ballots to recount. Current VVPAT alternatives include optical scan machines and supplementing DRE machines with DRE printers.

  Studies have repeatedly shown that optical scan systems have lower up-front costs than DREs, but that ballot printing costs may make DREs the less expensive option if they remain in use beyond about 20 years. Other studies have refuted the idea that DREs ever become cost-competitive with optical scan systems, showing that DREs do not last for 20 years and that many more DREs per precinct are required compared to optical scan counting machines to provide adequate access to voters.

- **Adopt VVPAT that can be counted by hand, as well as by machine—machine tallies to support prompt reporting of results with hand counting for audit and recount purposes.** Experience thus far with attaching printers to DREs has been unsatisfactory, mainly because of readability. Vendors are working on better systems, but they are still in the planning and experimental stages. If

DRE printers are adopted, care should be taken to ensure that they will support hand counting. Hamilton and Pickett Counties currently use optical scan systems countywide for most voters and have DREs for disabled voters. Ballot marking devices that can be used by disabled voters to mark their optical scan ballots in privacy, print them, and put them in the ballot boxes like all other voters are available.

- **Adopt a standard for VVPAT that would meet federal guidelines under consideration.** While staff concludes that waiting for Congressional action is not advisable, it would be unwise to ignore the standards likely to emerge if Congress passes a bill. These standards cannot currently be met by DRE printers. If such printers were purchased and Congress passed the "Holt bill" or the "Feinstein bill," the new printers would have to be discarded. No requirements are under serious consideration in Congress that would preclude the use of precinct-level optical scan systems.

- **Request a review by the Election Assistance Commission to find out how much of Tennessee's remaining HAVA funds would be available to purchase new voting machines.** When Florida's current Governor Charlie Crist asked the state legislature to require optical scan machines in all precincts in the state, he requested that the EAC allow him to spend some of Florida's remaining HAVA funds on the change. In a written response, Juliet T. Hodgkins, General Counsel for the EAC, stated that counties which had already used HAVA funds to replace their voting machines could not do so again. The EAC review found that some of Florida's HAVA funds could be used, but the reasons were very situation-specific. Tennessee should request a similar review so the state knows the full funding situation.

- **Require voting machine vendors to escrow all of their proprietary software so that it can be reviewed by experts as recommended by the Commission on Federal Election Reform and secured for further analysis <u>if vote-counting problems should arise</u>.** The inability to study

the software when there are questions about an election with no paper records seriously undermines confidence in the results of recounts and audits. Elections are the basis of democracy, and it is not acceptable for a private interest to shield a part of the election process from the voters those private interests serve. Taxpayer dollars buy the voting machines and the software, and taxpayers have the right to ensure that their investment will produce reliable results. The source code is the actual counter of votes, and that counting must be more open if the public is to accept close election outcomes. Vendors may have valid concerns about proprietary software, and those concerns should be addressed as much as practicable, but at the very least, source code must be available for inspection by someone who is not in the vendor's employ when an election is close and in question. Inspectors could be limited to a small number of qualified people, and they can be required to sign non-disclosure agreements. Having a copy of the source code as delivered by the vendor would provide protection to vendors as well. In the event that the code was altered after delivery, vendors would have an official record of the code as they delivered it. A process that would allow for open examination of source code is desirable and should be explored for the future. One possibility is using voting machines with all open source code programs.

- **Strengthen audit requirements to ensure that a random sample of machines is routinely tested by comparing hand counts to machine totals, and when results vary by more than a small percentage, that a broader recount process follows.** Numerous studies have demonstrated that machine counters can be programmed, maliciously or negligently, to miscount. Small miscounts might not create enough suspicion to prompt a recount, especially in a statewide or national race in which individual counties do not get much notice. But systematic small miscounts can change the outcome in any close race. Governmental entities and private corporations are routinely audited

regardless of whether problems are suspected. With so much a stake, the same should be true for elections.

In most states that require audits, a small number of precincts are randomly chosen to recount their ballots fully. Any discrepancies are investigated. If satisfactory explanations cannot be found, then all precincts will recount. Some states randomly select a percentage of ballots in all precincts and recount them manually. Any recount totals that do not fall within a specified margin of error for the overall precinct total trigger a wider recount. As an alternative, several states have an automatic partial or full recount only when a race is very close (generally when the top two candidates are within a point or two of each other). The State of Minnesota enacted a post-election review law in 2004 to assess the accuracy of its voting machines. If the audit reveals a difference greater than 0.5%, a broader audit is automatically triggered.

- **Consider making early voting and voting by mail more accessible.** Broadening the availability of both would reduce the pressure on polling places on election day, addressing one of the concerns of recent elections—long lines and long waits. Voting early has proven quite popular where it is widely available. In Tennessee, nearly 50% of the statewide November 2006 vote was cast early. Some Tennessee legislators have reported receiving complaints about the lack of access to early voting by those outside of cities. It should be a real option for rural voters as well as for urban ones. More locations and a longer early voting period are options to consider. Voting by mail is essentially absentee voting. Tennessee requires a reason for voting absentee. Most states do not. Allowing anyone who wishes to vote absentee would increase voting opportunities. There is reason to believe it would increase voter turnout while taking some of the pressure off of polling places that can result in long lines on election day.

- **Consider a Vote by Mail pilot program that would allow the state to assess the advantages and disadvantages of this type of voting in Tennessee.** The success and

acceptance of voting by mail in states like Oregon and Washington suggests that it is worth further investigation. Voting by mail creates its own paper trail, solving the problem most DREs pose for recounts and audits, but it may create other problems. Potential benefits include decreased expense and higher turnout. The Joint Study Committee on the Voter Confidence Act of 2006 recommended a pilot program, and a bill currently in Congress would fund such a program if it passes. Given the potential to increase voter turnout, a pilot program in Tennessee might be desirable regardless of whether federal funding becomes available.

- **Strengthen security and pre-test requirements and make them consistent for all voting systems.** The testing requirements for different types of voting systems are not consistent, and there is much that is out-of-date and no longer applies. While this is not necessarily critical to fair elections, it does need to be done at some point.

- **Consider election day parallel voting machine tests to detect hidden programs that are triggered by election day conditions and are erased so that they cannot be detected later.** Several jurisdictions, including at least one state, choose voting machines at random on election day, remove them from use, put them on public display, and use them to test the equipment and software to ensure that nothing that happens during the day affects vote counts. A series of predetermined ballots are cast on the test machines periodically throughout the day; totals for each machine are checked at the end of the day to make sure all ballots were counted correctly. These tests measure the election day performance of the machines and ensure that they do not have hidden programs that activate only on election day and cause miscounts. The State of Maryland used this process in 2004, casting 1,300 ballots to test the reliability of their machines. If optical scan were to be adopted statewide, most counties would have only one counting machine per precinct. Parallel tests could still randomly select at least one machine per county to test openly on election day.

ENDNOTES

[1] Zogby International 2006.

[2] Sewell 2007.

[3] National Association of Secretaries of State 2004.

[4] See, for instance, Myerson 2005 and McCloy 2005.

[5] McCloy 2005.

[6] Moore 2006.

[7] *The New York Times* 2004.

[8] VotersUnite.org 2006.

[9] See a full list of early and absentee voting laws by state at http://electionline.org/Default.aspx?tabid=474

[10] Gronke 2005, 2.

[11] Gronke 2005, 7-8.

[12] Stein, Leighley, Owens 2005, 7-8.

[13] Washington Office of the Secretary of State 2006a and 2006b.

[14] Lin 2007.

[15] See 17 USCA § 101, SecureInfo Corp. v. Telos Corp 387 F. Supp. 2d 593 (E.D. Va. 2005) and TCA Title 47, Chapter 25, Part 17.

[16] Commission on Election Reform 2005, 29.

[17] Wagner, David 2007, 11.

[18] Matt Zimmerman, attorney for the Electronic Frontier Foundation, phone interview, February 21, 2007.

[19] Commission on Election Reform 2005.

[20] Kropko 2007.

[21] Electionline.org 2007.

[22] Rules of the Tennessee Department of State Chapters, 1360-2-12 and 1360-2-13.

APPENDICES

APPENDIX A

CONCERNS REGARDING SHELBY COUNTY DIEBOLD GEMS CENTRAL TABULATOR ADMINISTRATION IN THE AUGUST 3, 2006 PRIMARY ELECTION

OVERVIEW OF GEMS TABULATOR SOFTWARE

This software can be installed on any standard PC with a Windows operating system.

The GEMS application is designed with two main pieces.

1) Graphic user interface file (view screens, buttons, reports, etc.)

2) Microsoft Access database .MDB file containing multiple tables where the actual vote totals are stored.

CRITICAL SECURITY BREACH

Not only was the main Diebold central tabulator found to be plugged into a county government network switch, the following unauthorized software had been installed on it:

1) Lexar Jump Drive encryption software.

    This would allow someone to manually transfer data between the tabulator PC and another PC using a small USB type "thumb" drive. Such drives have the capacity easily to hold the above Microsoft Access database file containing Shelby County's primary election vote totals.

2) PC Anywhere

    This application would allow unfettered remote access to the central tabulator to anyone connected to the county government network or the Internet.

3) Microsoft Office Professional (which includes Microsoft Access)

    This would allow manual editing of the Diebold GEMS database file, which is NOT password protected and bypassed by the GEMS audit logs. In fact, the "AuditLog" table itself can easily be edited. Vote totals can be altered in the "CandidateCounter" table much like editing a spreadsheet. Or, the candidate names can simply switched in the "Candidate" table.

4) HTML editor software

    This indicates someone was attempting to edit saved Diebold election

summary reports, perhaps to agree with altered vote totals in the Diebold Microsoft Access database file.

CONCLUSION

Independent of voter concerns about trusting their ballot to paperless DREs, the real threat for wholesale election fraud lies with the Diebold central tabulator. If the DREs and optical scanners represent voter district "ATMs" the GEMS central tabulator is the county's "Bank".

Unless Shelby County election officials can be seen as conducting a good faith investigation as to who had access to this central tabulator PC and the above unauthorized software and who actually did the illegal install, voters in this county (and ultimately the state) can have no confidence in the integrity of the November 2006 election.

ACTIONS NEEDED

- The GEMS central tabulator should absolutely NOT be connected to any network via Ethernet card, wireless network card, infrared port, USB port or modem.

- The administrator password should be changed immediately and all other user accounts with rights to install software should be deleted from the Windows Local Security Policy.

- The unauthorized software, including the Lexar Jump Drive encryption software, PC Anywhere,

- Microsoft Office Professional, and the HTML Editor software, needs to be removed **immediately** from the GEMS central tabulator.

- Just before the polls open and immediately after the polls close, all central tabulators need to be audited, especially in the Windows event logs, for the existence of unauthorized software.

- From now until after the election results are certified, all central tabulators need to be physically protected from unsupervised access by any individual, including Diebold and other voting equipment vendors. This would **especially** include the installation of any last minute software "patches" and/or hardware upgrades.

APPENDIX B

2006 Election Day Incident Reports

	Machine Errors	Paper Errors	ID Required	Human Errors	Delays	Communication and/or training problems	Out of Ballots	Lack of Translators and/or Handicap Accessible	Fraud
Alabama	X	X		X					
Alaska		X		X					
Arizona			Very Few Problems						
Arkansas	X	X		X	X				
California	X	X		X					
Colorado	X				X				
Connecticut	X				X	X			
Delaware						X			
District of Columbia						X			
Florida	X	X		X	X	X			
Georgia			X		X	X			
Hawaii		X		X	X	X			
Idaho	X	X		X	X	X			
Illinois	X				X				
Indiana	X		X			X			
Iowa	X			X	X				
Kansas	X				X				
Kentucky					X				
Louisiana									
Maryland	X				X				
Massachusetts			X		X		X	X	
Maine	X				X				
Michigan				X	X		X		
Minnesota	X				X	X			
Mississippi									
Missouri	X		X		X			X	
Montana					X				
Nebraska	X								
Nevada	Have used touch screens for several elections								

APPENDIX B (CONTINUED)

	Machine Errors	Paper Errors	ID Required	Human Errors	Delays	Communication and/or training problems	Out of Ballots	Lack of Translators and/or Handicap Accessible	Fraud
New Hampshire	Used vote by phone for voters with disabilities								
New Jersey	X				X				X
New Mexico								X	
New York					X				
North Carolina									
North Dakota									
Oklahoma	X				X				
Ohio	X		X		X				
Oregon					X				
Pennsylvania	X				X				
Rhode Island	X				X				X
South Carolina	X		X	X	X	X			
South Dakota	X						X		
Tennessee	X				X				
Texas	X	X							
Utah					X				
Vermont		X							
Virginia						X			
Washington	Weather Problems								
West Virginia	X								
Wisconsin			X						
Wyoming									
Total	26	9	7	10	28	11	3	3	2

NOTE: In only two states were fraud charges raised, New Jersey and Rhode Island. In New Jersey more than 20 voters reported receiving ballots that had already been marked for a particular candidate. In Rhode Island a local newspaper reported that 5,000 dead people are registered to vote in the state. The Secretary of State's office began checking the voter rolls. Source: Election Reform Information Project (www.electionline.org)

In 2004, the "Beacon Journal", Cleveland, Ohio reported that two election workers were convicted of illegally rigging the 2004 presidential election recount because they did not randomly select ballots in the recounting process.

APPENDIX C

SUMMARY OF COMMENTS CONCERNING VOTING MACHINES OF PRESENTERS AT THE SEPTEMBER TACIR MEETING

Jeff COLLINS from Harp Enterprises said that his company merely sells and services Hart machines in Tennessee and introduced Travis HAROLD of Hart Intercivic to talk to the commissioners about that company's voting machines. Mr. HAROLD presented a history of his company and the development of their DREs and discussed the California Secretary of State's findings relative to Hart DREs in California's recent top-to-bottom review. He said that they are not aware of any vote ever having been lost on their system. He said that their system is secure and that more security is always possible but requires more money.

Senator KURITA asked how they would be aware if votes had been lost. After some follow-up, Mr. HAROLD's explanation was that sometimes there are problems, but there are procedures to deal with them, and, as far as they are aware, all votes have been recovered when there is a problem. Senator KURITA asked whether the voter or the contract holder is considered to be the customer. Mr. HAROLD replied that the contract holder is the customer. Senator KURITA asked about a statement he had made about not disclosing some problems to the public. Mr. HAROLD said that he meant that companies should have a chance to correct problems before disclosing them to the public to protect the system.

Mayor ROWLAND asked if Hart was the only voting machine to be recertified in California after the top-to-bottom review. Mr. HAROLD stated that they were the only DRE to be fully recertified. John JOHNSON asked what percentages of voters in California and Tennessee would have voter verified paper audit trails by 2008. Mr. HOWARD said that such a paper trail is required in California so they would have it, but that Tennessee does not require it and does not have it.

Chairman RINKS asked Brook THOMPSON, Coordinator of Elections to come forward for a question and asked him how the vendor certification process works in Tennessee. Mr. THOMPSON said that both he and the State Election Commission must certify voting equipment. He said that Tennessee requires federal certification before they will consider voting equipment here, and that Tennessee has additional processes it goes through prior to certification, such as seeing the equipment's use demonstrated.

John JOHNSON asked about voter verified paper audit trails in Tennessee. Mr. THOMPSON said that there was no federal certification process when DREs were originally certified in Tennessee, and that, though they had subsequently been federally certified, his office had concerns about maintaining voter anonymity and quality of the printers. He

said that precinct-based optical scan would be a better choice for Tennessee if the state requires voter verified paper audit trails. He pointed out, though, that such machines make early voting more complicated because many different kinds of ballots must be printed.

Alderman KIRK asked about how counties' purchase decisions affect certification, and Mr. THOMPSON said counties can use any certified machines but that their decisions do not affect certification.

Senator KURITA asked why early voting would be negatively impacted by precinct-based optical scan. Mr. THOMPSON explained that optical scan requires printed ballots and many different ballots are needed for early voting sites. Senator KURITA pointed out that there are ways to make it easier, like having every precinct open for early voting. Mr. THOMPSON pointed out some problems with that, but agreed that if the legislature wants such a system, there are ways to overcome some problems.

Mayor BRAGG asked about the difficulty of finding places to vote, especially in the states roughly 20 urbanized areas. Mr. THOMPSON said the security issues make schools more difficult to use, and that is true in all areas, not just the urbanized ones. Mr. THOMPSON said that many people will tell you that the best thing we could do is close schools on election day so student security is not an issue, use the schools as polling places and the teachers as poll workers (state, county, and municipal government workers cannot currently work at the polls in Tennessee).

Jimmy RIES, President of Microvote General Corporation, gave a brief history of Microvote and its business in Tennessee. He pointed out that all technologies have their own weaknesses, and optical scan still provides the voter no proof that their votes counted as marked. He also pointed out that the Americans with Disabilities organization is against paper balloting of any kind because it puts their voters at a disadvantage. He also mentioned Ballot on Demand systems, which allow poll workers to print the correct ballot from a DRE when a voter requests it rather than having to have them all pre-printed.

Representative Larry TURNER asked if anonymity was compromised when a printer was added to a DRE as has been suggested. Mr. RIES said that there were ways to address that, by having the record cut off and drop into a ballot box after each voter was finished. Representative Turner asked if Mr. RIES had suggested that the scanning process is no more accurate than the touch screen process. Mr. RIES said that he had only said that optical scan lacked voter verification as well. Chairman RINKS pointed out that the paper ballot offers the opportunity to recount.

Dr. GREEN asked how many generations of voting machines we will go through before we get one that we can keep? He pointed out that we spend $70 billion on a single voting system and that voting is very important and why can we not have a system that we have confidence in. Mr. RIES said that we probably should have had this debate before the new machines were bought.

Cathy ROGERS of Premier Voting Systems (formerly Diebold) presented next. She talked about ongoing research and ways that voter verifiability might be addressed in the future. She defended thermal paper printers. She talked about the length of time it takes to make changes in voting systems, and she discussed the fact that all voting systems are subject to fraud. She also pointed out that tests on voting machine security do not take place in real-world election conditions.

Representative YOKLEY asked how long the timeline would be for switching to optical scan. Ms. ROGERS said that there are already machines that meet the 2002 standards, but there may be a wait for the 2005 standards. She also said that optical scan is a good technology as well as DREs.

Nathan RIDLEY from Elections Systems & Software gave background on his company and talked about the Help America Vote Act and the problems it was meant to address, including the much more equal access DREs have given to disabled voters. His also made the point that it is getting late to make changes for 2008, and that access to early voting and ballot secrecy issues should be considered. He mentioned some possible improvements to the system, including reducing the number of precincts, paying poll workers more, and making registration easier. He said that our election process is still set up on the idea of a one day election while early voting makes an election period more applicable. Chairman RINKS agreed that the whole process should be examined, including election periods rather than election days and central voting locations.

Dr. Dan WALLACH discussed the top-to-bottom review in California that he participated in and said that voting systems simply weren't designed with security in mind and that the regulatory framework has been insufficient. He said that there were many ways to approach the problems, but that voter confidence in the outcome could not be achieved without improvements and that there are currently not good processes in place to catch mistakes. He also said that trade secrets should have no place in voting technology.

Dr. GREEN asked what can be done to ensure security of voting machines. Dr. WALLACH said that, in the short term, he would recommend limiting the use of DREs to one per precinct for disabled voters and use optical scan with ballot on demand systems. In the long term, he and his colleagues are working on secure DREs. Senator Jim TRACY asked if there was proof that an election had ever been hacked. Dr. WALLACH said there was

not, but there were irregularities that could have been hacking, in addition to the fact that good hacking would be hard to detect.

Dick WILLIAMS of Common Cause introduced Bernie ELLIS, of Gathering to Save Our Democracy, an organization that Common Cause has partnered with on this issue. Mr. ELLIS said that Tennessee has led the way in voting rights in the past and that this was something to be proud of. He pointed out some serious irregularities in some recent election that may not be able to be proved as fraud but that point to the need to be able to do recounts and audits. He described problems in many states and said that optical scan with ballot on demand was his organization's recommendation. He likened DREs to Astroturf in that the idea sounded good at first but turned out to have many unforeseen problems so serious that it just wasn't usable.

Mayor ROWLAND asked Mr. ELLIS' opinion on voting by mail, and he replied that TACIR staff's recommendation to try a pilot program seemed a good one.

Dr. GREEN pointed out that the information published so far has been a result of staff's research and that the Commissioners have not yet taken a position on any of these issues.

Chairman RINKS said he would like to hear from county election representatives at the next meeting to see what they think of these issues and what they see as problems if changes are made. He directed staff to work with Brook THOMPSON to set that up.

APPENDIX D

DEBRA **B**OWEN
CALIFORNIA SECRETARY OF STATE
NEWS RELEASE

Frequently Asked Questions
About Secretary of State Debra Bowen's
Top-To-Bottom Review of California's Voting Systems

Revised August 15, 2007
To view prior versions of this FAQ, please click here.

The Secretary of State released her decertification and recertification orders on August 3, 2007. What do those orders mean?
The Secretary of State decertified the following voting systems on August 3, 2007:

- Diebold GEMS 1.18.24/AccuVote TSX/AccuVote-OS
- ES&S InkaVote Plus Precinct Ballot Counter Voting System, version 2.1
- Hart Intercivic System 6.2.1
- Sequoia WinEDS version 3.1.012/Edge/Insight/400-C

She then recertified all but one system (the ES&S InkaVote Plus Precinct Ballot Counter Voting System, version 2.1) with a number of conditions. A detailed list of all of the conditions for each system can be found by **clicking here**, but in brief, the conditions require:

- Counties that use any one of the six systems must adopt security procedures detailed in the recertification documents.
- For counties using direct recording electronic (DRE) machines made by Sequoia and Diebold, no more than one such machine may be used per polling location on Election Day. Elections officials must conduct a 100% manual count of the voter-verified paper audit trail (VVPAT) for votes cast on those machines.
- All six systems will be subject to increased post-election audits to ensure election results are accurately tabulated.

How will counties and voters be affected by this decision?
Nearly nine million California voters cast ballots in the November 2006 gubernatorial election and over 75% of them voting using either a paper-based absentee ballot or a paper-based optical scan ballot.

Of California's 58 counties, 35 of them rely primarily on a paper-based optical scan system for their Election Day balloting. Most of them use one DRE in each polling place to comply with the Help America Vote Act (HAVA) requirement to enable voters with disabilities to vote privately and independently. These counties will have to comply with a number of security and post-election audit requirements, but by and large, voters in these counties won't see any change when they go to the polls on Election Day.

Two counties rely on the Hart Intercivic DRE for their polling place voting system. These counties will have to comply with a number of security and post-election audit requirements, but by and large, voters in these counties won't see any change when they go to the polls on Election

Day.

Twenty-one counties rely on either the Sequoia Edge I, the Sequoia Edge II, or the Diebold TSx DRE systems for their polling place system. Except for the single DRE allowed per polling place, these counties will have to adopt a new Election Day voting system. It is in these 21 counties where voters will notice the biggest change on Election Day.

For a list of voting systems by county, please **click here**.

Why wasn't the InkaVote Plus voting system recertified?
ES&S, the provider of the InkaVote Plus system, didn't provide the equipment and information necessary for that system to be included in the review in a timely fashion. The Secretary of State intends to put this system through the same rigorous testing process the other systems in the top-to-bottom review process were subjected to. Depending on the results of the review, that system may be recertified in time for it to be used in the February 2008 presidential primary election.

How much did the review cost and where did the funding come from to pay for it?
Approximately $450 million has been spent or set aside to upgrade California's voting equipment over the past several years.

The total cost of the top-to-bottom review was originally estimated to be $1.8 million, but because fewer systems were reviewed than was anticipated, the cost to date has been $905,000.

A portion of the money used to conduct the review came from the $760,000 in federal HAVA funding that was provided by the Legislature for voting machine source code review as part of the 2006-07 state budget. The remaining funding for the review came from the voting system vendors. It's estimated the review of each system cost approximately $262,000, with the costs being split equally between the vendor and California's HAVA funding allocation. California law, as well as the certification agreements many of the voting system vendors signed with the former Secretary of State, allow the Secretary of State to review voting systems at any time and allow the Secretary of State to require vendors to pay for the cost of conducting the review.

Why was it necessary to conduct a top-to-bottom review of California's voting systems?
The top-to-bottom review was designed to give California's voters an answer to one simple question: Are all of California's voting systems secure, accurate, reliable and accessible?

Furthermore, Elections Code Section 19222 requires the Secretary of State to review the voting systems Californians are asked to cast their ballots on, stating:

> The Secretary of State shall review voting systems periodically to determine if they are defective, obsolete, or otherwise unacceptable. The Secretary of State has the right to withdraw his or her approval previously granted under this chapter of any voting system or part of a voting system should it be defective or prove unacceptable after such review. Six months' notice shall be given before withdrawing approval unless the Secretary of State for good cause shown makes a determination that a shorter notice period is necessary. Any withdrawal by the Secretary of State of his or her previous approval of a voting system or part of a voting system shall not be effective as to any election conducted within six months of that withdrawal.

2

What is a top-to-bottom review of California's voting systems?

The top-to-bottom review consisted of a thorough examination of all voting system documentation, procedures and the equipment used to record and tally votes. The review had four components:

- ❑ A document review examined manufacturer documentation, testing reports from federal Independent Testing Authorities (ITAs), reports from prior state certification testing, and reports of independent examinations and testing of voting systems.

- ❑ A source code review examined the human-readable instructions that are converted into machine-readable code to run the voting systems. The primary focus was to identify any security vulnerabilities that could be exploited to alter vote recording, vote results, critical election data such as audit logs, or to conduct a "denial of service" attack that prevents people from voting.

- ❑ Red team penetration testing involved open-ended, hands-on efforts to identify and document any potential for tampering or error in any part of the voting system's hardware, storage devices or software.

- ❑ The accessibility of the voting systems was assessed and included test voting on each of the voting systems by volunteer voters representing a broad range of disabilities.

The document review teams, source code review teams and red teams interacted regularly to learn from one another and to ensure the review of all systems is even-handed.

How were the voting systems evaluated and did that differ from the draft criteria published on March 22?

The draft criteria was an initial proposal for discussion and public input. Based on the substantial number of comments received, the final project plan used to evaluate the voting systems didn't include those draft standards. Instead, the top-to-bottom review teams provided an independent technical evaluation of the voting systems that the Secretary of State used to carry out her statutory duty with respect to voting systems, as required by Division 19 of the State Elections Code.

The standards and definitions for security, accuracy, reliability and protection of ballot secrecy governing the top-to-bottom review are set forth in the federal 2002 Voluntary Voting System Standards, which may be found at http://www.eac.gov/election_resources/vss.html. California Elections Code Section 19250 requires voting systems to comply with these standards as a condition of being certified for use in the state.

With respect to accessibility for voters with disabilities and with alternative language requirements, the standards and definitions governing the top-to-bottom review are set forth in the 2005 federal Voluntary Voting System Guidelines, which may be found at http://www.eac.gov/VVSG%20Volume_I.pdf and in California Elections Code Sections 19227, 19250 and 19251.

<div align="center">3</div>

The red team penetration testing was conducted in accordance with Resolution # 17-05 of the Technical Guidelines Development Committee (hereafter "TGDC") of the U.S. Election Assistance Commission, adopted at the TGDC plenary meeting on January 18-19, 2005, which calls for:

> ". . . testing of voting systems that includes a significant amount of open-ended research for vulnerabilities by an analysis team supplied with complete source code and system documentation and operational voting system hardware. The vulnerabilities sought should not exclude those involving collusion between multiple parties (including vendor insiders) and should not exclude those involving adversaries with significant financial and technical resources."

Who conducted the review?
The Secretary of State contracted with the University of California (UC) to assemble three top-to-bottom review teams that relied on specialists from UC, as well as from public and private universities and private sector companies throughout the United States. To ensure a fresh look at the voting systems, scientists with specific experience in voting system technology and security experts from other fields who had no experience with voting system technology were asked to participate. Each review team consisted of at least seven members and included three components – document review, source code review, and red team penetration testing.

❑ The two Principal Investigators for the project were Matthew Bishop, Professor in the Department of Computer Science and Co-Director of the Computer Security Laboratory at UC Davis, and David Wagner, Associate Professor in the Computer Science Division at UC Berkeley, with extensive experience in computer security, cryptography and electronic voting. David Wagner is a founding member of the ACCURATE center, which is funded by the National Science Foundation to research ways that technology can be used to improve voting.

The accessibility of the voting systems was assessed by a single team of two accessibility experts, headed by Noel Runyan, an electrical engineer and computer scientist with over 33 years experience in designing and manufacturing access technology systems for people with disabilities. The accessibility assessment included test voting on each of the voting systems by volunteer voters representing a broad range of disabilities.

For a complete listing of team members, as well as resumes, biographies, and/or curriculum vitaes, please **click here**.

What if a voting system vendor chose not to participate in the review?
If a vendor chose not to have its voting system reviewed, the Secretary of State had the option of initiating a decertification process immediately. The Secretary of State could also impose conditions on the use of such systems, even though they had not been through the top-to-bottom review, in the event a vendor would like to have a county use such a system in 2008.

What happens with new voting systems that receive federal approval?
If a system received federal approval and was submitted to the Secretary of State by July 1, 2007, for certification in California, the Secretary of State will fully review that system using the same standards that were applied in the top-to-bottom review.

4

What if a vendor opted out of having its existing system tested in anticipation of federal approval later this year for a replacement system?
Any system that was not federally certified and submitted to the Secretary of State by July 1, 2007, will not have sufficient time to complete the state certification process before the February 2008 election. Therefore, if a vendor opted out of the top-to-bottom review but did *not* submit a replacement system for certification by July 1, 2007, the Secretary of State may either decertify or conditionally recertify the existing system for 2008 elections with additional restrictions.

Did the top-to-bottom review test entire voting systems or only the voting machines used in polling places?
The only way to make sure a voting system is properly recording and counting votes is to review a voting system from top to bottom. That's why the review included all of the various machines used to *cast* ballots, as well as the systems used to *count* ballots, including vote tabulating devices, election management and tabulation programs, and associated firmware, software and peripheral devices.

What systems were tested?
The following certified voting systems were examined and tested under the top-to-bottom review:

Diebold GEMS 1.18.24/AccuVote
- GEMS software, version 1.18.24
- AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4
- AccuVote-OS (Model D) with firmware version 1.96.6
- AccuVote-OS Central Count with firmware version 2.0.12
- AccuFeed
- Vote Card Encoder, version 1.3.2
- Key Card Tool software, version 4.6.1
- VC Programmer software, version 4.6.1

Hart Intercivic System 6.2.1
- Ballot Now software, version 3.3.11
- BOSS software, version 4.3.13
- Rally software, version 2.3.7
- Tally software, version 4.3.10
- SERVO, version 4.2.10
- JBC, version 4.3.1
- eSlate/DAU, version 4.2.13
- eScan, version 1.3.14
- VBO, version 1.8.3
- eCM Manager, version 1.1.7

Sequoia WinEDS version 3.1.012/Edge/Insight/400-C
- WinEDS, version 3.1.012
- AVC Edge Model I, firmware version 5.0.24
- AVC Edge Model II, firmware version 5.0.24

5

- VeriVote Printer
- Optech 400-C/WinETP firmware version 1.12.4
- Optech Insight, APX K2.10, HPX K1.42
- Optech Insight Plus, APX K2.10, HPX K1.42
- Card Activator, version 5.0.21
- HAAT Model 50, version 1.0.69L
- Memory Pack Reader (MPR), firmware version 2.15

Were any systems not reviewed by the Secretary of State s part of the top-to-bottom review?
The DFM Mark-A-Vote system used by Lake, Madera, and Sonoma counties was not reviewed in this round of testing, but the Secretary of State reserves the right to conduct a review of this system at a later date.

The Opto-Mark system, operated by Martin & Chapman Company and used in several cities to conduct local elections, was not reviewed in this round of testing, but the Secretary of State reserves the right to conduct a review of this system at a later date.

The Votec system, used by the City of Los Angeles to conduct local elections, was not reviewed in this round of testing, but the Secretary of State reserves the right to conduct a review of this system at a later date.

ES&S declined to submit its Unity 2.4.3.1/AutoMARK and its City and County of San Francisco Voting System to the top-to-bottom review because it doesn't intend to have any county use those systems in 2008. Should ES&S attempt to have a county use those systems, the Secretary of State has the right to attach additional use conditions to the systems pursuant to the 2006 certification of the systems, regardless of the fact that they weren't submitted for inclusion in the top to bottom review.

As noted earlier in this document, ES&S didn't submit its InkaVote Plus Precinct Ballot Counter Voting System, version 2.1, in time for it to be included in the review, despite the fact that the sole California user of this system – Los Angeles County – intends to use the system in 2008. As a result, the Secretary of State has decertified the system, but intends to conduct a review of this system soon and has the right to recertify it depending on the results of that review.

Hart Intercivic declined to submit its System 6.1 to the top-to-bottom review because it doesn't intend to have any county use that system in 2008. Instead, Hart Intercivic has voluntarily opted to decertify that system, meaning the Intercivic System 6.1 won't be used by any city or county in 2008.

Los Angeles County declined to submit its Microcomputer Tally System (MTS) version 1.3.1 to the top-to-bottom review because it intends to move to an alternate system in 2008. Should it decide to use the system in 2008, the Secretary of State has the right to attach additional use conditions to the system, regardless of the fact that it wasn't submitted for inclusion in the top-to-bottom review. A link to a letter detailing Los Angeles County's decision not to submit its system to the top-to-bottom review can be found **here**.

6

Where was the top-to-bottom review being conducted?
Testing, examination and review activities, and analysis were conducted onsite at the Secretary of State's facilities in Sacramento under secure conditions, with one exception. The review of documentation and source code was, upon express written authorization of the Secretary of State, conducted at secure facilities of UC or other secure locations designated by UC.

Was this review open to the public?
Given the proprietary nature of the systems being reviewed and the legal requirements to protect the intellectual property of the vendors, the ability to conduct the review in a completely public fashion was severely constrained. However, the Secretary of State created a public observation room that allowed any member of the public to watch the review process via the security cameras that were set up in the testing facility. The Secretary of State maintained an updated telephone hotline to allow anyone to call in and find out what the testing schedule was for the following day, so they could determine if they wanted to come to the public observation room to view it.

How can I read the reports prepared by the independent UC review teams?
You can **click here** to get back to the main Top-To-Bottom Review Page, where you'll find copies of the UC top-to-bottom review reports and more information about the entire top-to-bottom review process.

7

BIBLIOGRAPHY

Ackerman, Kenneth D. 2005. *Boss Tweed: The rise and fall of the corrupt pol who conceived the soul of modern New York.* New York, NY: Carroll and Graf.

Allen, Howard W. and Kay Warren Allen. 1981. Vote fraud and data validity. In *Analyzing electoral history: A guide to the study of American voter behavior*, by Jerome M. Clubb, et al. Beverly Hills, CA: Sage.

Alvarez, R. Michael and Thad Hall. 2005. *The next big election challenge: Developing electronic data transaction standards for election administration.* Pasadena, CA: California Institute of Technology and Massachusetts Institute of Technology, Voting Technology Project.

Avrich, Paul. 1984. *The Haymarket Tragedy.* Princeton, NJ: Princeton University Press.

Baumgardner, James L. 1984. The 1888 presidential election: How corrupt? *Presidential Studies Quarterly* 14.

Bederson, Ben et. al. 2005. *The need for usability of electronic voting systems: Questions for voters and policy makers.* New York, NY: Association of Computing Machinery.

Bensel, Richard Franklin. 2004. *The American ballot box in the mid-nineteenth century.* Cambridge, MA: Cambridge University Press.

Blair, A.Z. 1911. Seventeen hundred rural vote sellers: How we disfranchised a quarter of the voting population of Adams County, Ohio. *McClure's Magazine*, November.

Bonner, Lynn. 2005. Voting machine maker leaves N.C. *newsobserver.com*, December 23. http://www.newsobserver.com/102/story/381151.html (accessed February 28, 2007).

Bradbury, Bill. 2005. Vote-by-mail: The real winner is democracy. *Washington Post*, January 1. http://www.washingtonpost.com/wp-dyn/articles/A40032-2004Dec31.html (accessed February 16, 2007).

Broache, Anne. 2005. North Carolina defends e-voting certifications. *CNETNews.com,* December 2. http://news.com.com/North+Carolina+defends+e-voting+certifications/2100-1028_3-5980671.html (accessed March 1, 2007).

Bucholz, Ron. 2004. *Accessibility and auditability in electronic voting.* San Francisco, CA: Electronic Frontier Foundation.

Burnham, Walter Dean. 1955. *Presidential ballots 1836-1892.* Baltimore: Johns Hopkins University Press.

———. 1965. The changing shape of the American political universe. *American Political Science Review* 59.

———. 1986. Those high nineteenth-century American voting turnouts: Fact or fiction? *Journal of Interdisciplinary History*, Spring.

Butler, Anne M. and Wendy Wolff. 1995. *United States Senate election, expulsion, and censure cases, 1793-1990.* Washington, D.C.: Government Printing Office.

Callahan, David. 2004. *The cheating culture: Why more Americans are doing wrong to get ahead.* New York, NY: Harcourt.

Callow, Alexander B. Jr. 1966. *The Tweed ring.* New York, NY: Oxford University Press.

Campbell, Tracy 2005. *Deliver the vote: A history of election fraud, an American political tradition- 1742-2004.* New York: Carroll and Graf Publishers.

————. 2003. Machine politics, police corruption, and the persistence of vote fraud: the case of the Louisville, Kentucky election of 1905. *Journey of Policy History* 15.

Celeste, Richard, Dick Thornburgh, and Herbert Lin, eds. 2005. *Asking the right questions about electronic voting.* Washington, DC: The National Academies Press.

Chang, Kenneth. 2001. From ballots to cockpits, questions of design. *New York Times*, January 23.

Cohen, Lizabeth. 2003. *A consumers' republic: The politics of mass consumption in postwar America.* New York, NY: Vintage.

Cohen, Norman S. 1968. The Philadelphia election riot of 1742. *Pennsylvania Magazine of History and Biography*, July.

Colorado Secretary of State. 2006. *State of Colorado security procedures for electronic voting systems.* Denver, CO. http://www.elections.colorado.gov/WWW/default/ Voting%20Systems/2006%20Security%20Plans/ Colorado%20County%20Security%20Procedures%20-FINAL.pdf (accessed February 26, 2007).

Commission on Election Reform. 2005. *Building confidence in U.S. elections.* Washington, DC: Center for Democracy and Election Management, American University. http:// www.american.edu/ia/cfer/ (accessed February 21, 2007).

Compuware Corporation. 2003. *Direct recording electronic (DRE) technical security.* Assessment report prepared for the Ohio Secretary of State.

Conley, Patricia Heidotting. 2001. *Presidential mandates: How elections shape the national agenda.* Chicago, IL: University of Chicago Press.

The Constitution Project's Forum on Election Reform. 2001. *Building consensus on election reform.* Washington, DC: Georgetown University Public Policy Institute.

Conyers, John, Congressman. 2005. *What went wrong in Ohio: The Conyers report on the 2004 presidential election.* Chicago, IL: Academy Chicago Publishers.

County of San Bernardino. 2004. *County on Tuesday will be first to use voter-verified paper trail.* San Bernadino, CA, October 29. http://www.co.sanbernardino.ca.us/pressreleases/ docs/981papertrailrelease10-29-04.pdf (accessed February 20, 2007).

Crenson, Matthew A. and Benjamin Ginsberg. 2002. *Downsizing democracy: How America sidelined its citizens and privatized its public.* Baltimore, MD: Johns Hopkins University Press.

Crozier, Michel, Samuel P. Huntington, and Joji Watanuki. 1975. *The crisis of democracy: Report on the governability of democracies to the trilateral commission.* New York: New York University Press.

Danese, Tracey E. 2000. *Claude Pepper and Ed Ball: Politics, purposes, and power.* Gainesville, FL: University Press of Florida.

Davenport, John I. 1881. *The election frauds of New York City and their prevention.* New York, NY: Privately printed.

Dershowitz, Alan M. 2001. *Supreme injustice: How the high court hijacked election 2000.* New York: Oxford University Press.

Dill, David and Will Doherty. 2004. *Electronic voting systems.* San Francisco, CA: Verified Voting Foundation.

Dorsett, Lyle W. 1968. *The Pendergast machine.* New York, NY: Oxford University Press.

Drew, Christopher. 2007. U.S. bars lab from testing electronic voting. *The New York Times*, January 4. http://www.nytimes.com/2007/01/04/washington/ 04voting.html?ex=1325566800&en=584c23012a3953b5&ei=5088&partner=rssnyt&emc=rss (accessed March 7, 2007).

Electionline.org. 2006a. *Early and absentee voting law.* Richmond, VA: Election Reform Information Project. http://electionline.org/Default.aspx?tabid=474 (accessed February 16, 2007).

———. 2006b. *Election preview 2006: What's changed, what hasn't and why.* Richmond, VA: Election Reform Information Project. http://electionline.org/Portals/1/Publications/ Annual.Report.Preview.2006.Final.pdf (accessed February 16, 2007).

———. 2006c. *The 2006 election.* Richmond, VA: Election Reform Information Project. http://www.electionline.org/Portals/1/Publications/EB15.briefing.pdf (accessed March 12, 2007).

———. 2007. *Case study: Auditing the vote.* Richmond, VA: Election Reform Information Project. http://www.electionline.org/Portals/1/Publications/FINAL%20EDR%20pdf.pdf (accessed April 9, 2007).

———. Undated. *Early and absentee voting laws (as of 7/26/06).* Richmond, VA: Election Reform Information Project. http://www.electionline.org/Default.aspx?tabid=474 (accessed March 12, 2007).

———. **Undated.** *V*oting systems 2006 (as of 9/26/06). Richmond, VA: Election Reform Information Project. http://www.electionline.org/Default.aspx?tabid=1099 (accessed March 12, 2007).

Election Science Institute. 2006. *DRE analysis for May 2006 primary Cuyahoga County, Ohio.* San Francisco, CA. http://utahcountvotes.org/docs/esi_cuyahoga_final.pdf (accessed February 21, 2007).

Election Systems & Software. 2007. *Election Systems & Software (ES&S) response to HDNet report.* Omaha, NE. http://www.essvote.com/HTML/news_room/nr_08142007.html (accessed November 16, 2007).

———. 2007. *Statement regarding letter from Election Assistance Commission, August 14, 2007.* Omaha, NE. http://www.essvote.com/HTML/docs/Statement_Letter_from_EAC.pdf (accessed November 16, 2007).

Election Technology Council. 2005. *Overview of independent voting system testing and certification process.* Sacramento, CA.

Ernst, Harry W. 1962. *The primary that made a president: West Virginia 1960.* New Brunswick, NJ: Eagleton Institute of Politics.

Evans, Eldon C. 1917. *A history of Australian ballot system in the United States.* Chicago: University of Chicago Press.

Fischer, Eric A. 2003. *Election reform and electronic voting systems: Analysis of security issues.* Washington, DC: Congressional Research Service.

Fischer, Eric and Kevin Coleman. 2005. *The direct recording electronic voting machine (DRE) controversy: FAQs and misperceptions.* Washington, DC: Congressional Research Service.

Fischer, Eric and Kevin Coleman. 2004. *Elections reform: Overview and issues.* Washington, DC: Congressional Research Service.

Frank, Thomas. 2000. *One market under God: Extreme capitalism, market populism, and the end of economic democracy.* New York: Anchor Books.

Fredman, L.E. 1968. *The Australian ballot: The story of an American reform.* Lansing, MI: Michigan State University Press.

Fund, John. 2004. *Stealing elections: How voter fraud threatens our democracy.* New York, NY: Encounter Books.

Gans, Curtis. 2004. Registration rises moderately battleground states lead the way independents gain most. *American University News*, October 28. http://spa.american.edu/ccps/files/File/csae/csae102804.pdf (accessed February 21, 2007).

———. 2006. Registration percentage unchanged from 2002 record percentage eschew major parties. *American University News*, November 2. http://spa.american.edu/spafiles/File/news/csae20071102.pdf (accessed February 21, 2007).

Gathering to Save our Democracy. 2006. *Nuts and bolts on paper ballots used with optical scan voting systems: Information from Hamilton County election specialist, Shannon DeFries.* Unpublished.

Gideon, John. 2006. *Cuyahoga officials attack their vendor—No not Diebold; Election Sciences Institute.* Malibu, CA: International Humanities Center, August 24. http://votetrustusa.org/index2.php?option=com_content&task=view&id=1705&Itemid=51&pop=1&page=0 (accessed February 21, 2007).

Governor's Select Task Force on Election Procedures, Standards, and Technology. 2001. *Revitalizing democracy in Florida.*

Graham, Sara Hunter. 1996. *Woman suffrage and the new democracy.* New Haven, CT: Yale University Press.

Greider, William. 1992. *Who will tell the people?: The betrayal of American democracy.* New York: Simon and Schuster.

Gronke, Paul. 2005. *Ballot integrity and voting by mail: The Oregon experience. A Report for the Commission on Federal Election Reform.* Washington, DC: Center for Democracy and Election Management, American University. http://www.sos.state.or.us/executive/CarterBaker.pdf (accessed February 18, 2007).

Gronke, Paul, Benjamin Bishin, Daniel Stevens, and Eva Galanes-Rosenbaum. 2005. *Early voting in Florida, 2004.* Washington, DC: American Political Science Association. http://earlyvoting.net/resources/EVIC.APSA.2005.pdf (accessed May 2, 2007).

Gronke, Paul, Eva Galanes-Rosenbaum, and Peter A. Miller. 2007. *Early Voting and Turnout.* Portland, OR: Early Voting Information Center and Reed College. http://earlyvoting.net/resources/ohio07.pdf (accessed March 14, 2007).

Grove, Jeff. 2004. ACM statement on voting systems. *Communications of the ACM* 47: 69-70.

Gumbel, Andrew. 2005. *Steal this vote: Dirty elections and the rotten history of democracy in America.* New York: Nation Books.

Hacking Democracy. 2006. Los Angeles: HBO Documentary Films.

Halvorson, Mark and Laura Wolff. 2007. *Report and analysis of the 2006 post-election audit of Minnesota's voting systems.* Minneapolis, MN: Citizens for Election Integrity.

Harris, Beverly. 2004. *Black box voting: Ballot tampering in the 21st century.* Renton, WA: Talion Publishing.

Harris, Joseph P. 1934. *Election administration in the United States.* Washington, D.C.: Brookings Institution Press (reissued 2006).

Hartmann, Thom. 2003. If you want to win an election, just control the voting machines. *Common Dreams Newscenter,* February 6.

Hawkins, Marlin with Dr. C. Fred Williams. 1991. *How I stole elections: The autobiography of Sheriff Marlin Hawkins.* Privately printed.

Haworth, Paul Leland. 1906. *The Hayes-Tilden disputed presidential election of 1876.* Cleveland, OH: Burrows Bros.

Hersh, Seymour. 1997. *The dark side of Camelot.* Boston, MA: Little, Brown.

Hill, Sarah. 2006. *Election fraud references.* Pasadena, CA: California Institute of Technology and Massachusetts Institute of Technology, Voting Technology Project.

Hill, Steven. 2002. *Fixing elections: The failure of America's winner takes all politics.* New York, NY: Routledge.

Hitchens, Christopher. 2005. Ohio's odd numbers. *Vanity Fair,* March.

Hite, Randolph C. 2007. *Elections: All levels of government are needed to address electronic voting system challenges.* Testimony before the Subcommittee on Financial Services and General Government, Committee on Appropriations, House of Representatives. Washington, DC: GAO-07-576T.

Hoffman, Ian. 2005. E-voting machines rejected: State says Diebold failures in massive mock election could translate to problems at polls. *Oakland Tribune*, July 29. http://www.votersunite.org/article.asp?id=5774 (accessed February 21, 2007).

Hofstadter, Richard. 1948. *The American political tradition.* New York, NY: Knopf.

Hodgkins, Juliet T. 2007. *Memorandum in reference to use of HAVA funds.* May 2, 2007.

Imai, Kosuke and Gary King. 2004. Did illegal overseas ballots decide the 2000 U.S. presidential election? *Perspectives on Politics* 2.

Imse, Ann. 2006. Big bar code backfire. *Rocky Mountain News*, November 14. http://www.rockymountainnews.com/drmn/elections/article/0,2808,DRMN_24736_5142404,00.html (accessed April 4, 2007).

Jefferson, David, Aviel Rubin, Barbara Simons, and David Wagner. 2004. Analyzing internet voting security. *Communications of the ACM* 47: 59-64.

Jim March Election Investigation. 2007. *Damage is horrifying.* Memphis, TN: Memphis Operation Election Integrity.

Kahl, Mary. 1983. *Ballot box 13: How Lyndon Johnson won his 1948 Senate race by 87 contested votes.* Jefferson, N.C.: McFarland Co.

Kallina, Edmund F., Jr. 1988. *Courthouse over White House: Chicago and the presidential election of 1960.* Orlando: University of Central Florida Press.

Karlan, Pamela S. 2001. Equal protection: *Bush v. Gore* and the making of a precedent. In *The unfinished election of* 2000, ed. Jack Rakove. New York, NY: Basic Books.

Kelsey, John. 2006. *Electronic independent dual verification—status report.* Presentation to the Technical Guidelines Development Committee, December 4 and 5, 2006.

Kerley, David. 2007. Florida Governor Crist endorses "paper trail" voting machines. a*bcnews.com*, February 2. http://abcnews.go.com/WNT/story?id=2845672 (accessed March 9, 2007).

Keyssar, Alexander. 1992. Right to vote. In *The Oxford companion to the Supreme* Court, ed. Kermit L. Hall. New York, NY: Oxford University Press.

———. 2000. *The right to vote: The contested history of democracy in the United States.* New York: Basic Books.

———. 2001. The right to vote and election 2000. In *The unfinished election of* 2000, ed. Jack N. Rakove. New York, NY: Basic Books.

Kiayias, A., L. Michel, A. Russell, and A. A. Shvartsman. 2006. *Security assessment of the Diebold Optical Scan Voting Terminal.* Storrs, CT: University of Connecticut Voter Center and Department of Computer Science and Engineering.

Kibrick, Robert. 2006. *Voter-verified paper record legislation.* Wilmington, DE: Verified Voting Foundation, June 29. http://www.verifiedvoting.org/article.php?list=type&type=13 (accessed February 16, 2007).

King, Ronald F. 2001. Counting the votes: South Carolina's stolen election of 1876. *Journal of Interdisciplinary History* 33.

Kleppner, Paul. 1982. *Who voted?: The dynamics of electoral turnout, 1870-1980.* New York, NY: Praeger.

Kornbluh, Mark Lawrence. 2000. *Why America stopped voting: The decline of participatory democracy and the emergence of modern American politics.* New York, NY: New York University Press.

Kropko, Mike. 2007. Two election workers convicted of rigging '04 presidential recount. *Akron Beacon Journal*, January 24. http://www.ohio.com/mld/beaconjournal/news/state/16536269.htm?template=contentModules/printstory.jsp (accessed April 9, 2007).

Krueger, Maynard C. 1928. Election frauds in Philadelphia. *National Municipal Review*, May.

Landesco, John. 1974. Election fraud. In *Theft of the city: Readings on corruption in urban America*, eds. John A. Gardiner and David J. Olson. Bloomington, IN: Indiana University Press.

Laskowsky, Sharon J., Marguerite Autry, John Cugini, William Killam, and James Yen. 2005. *Improving the usability and accessibility of voting systems and products.* Gaithersburg, MD: National Institute of Standards and Technology Special Publication 500-256.

Lin, Judy. 2007. Mail voting gets election clerks' stamp of approval - others wary. *Sacramento Bee*, February 20. http://www.sacbee.com/111/story/125798.html (accessed February 20, 2007).

Longley, Lawrence D. and Neal R. Peirce. 1996. *The electoral college primer.* New Haven, CT: Yale University Press (updated 1999).

March, Jim. 2006. *Declaration of James "Jim" March.*

Mayfield, Loomis. 1993. Voting fraud in early twentieth century Pittsburgh. *Journal of Interdisciplinary History* 24.

McCormick, Richard P. 1953. *The history of voting in New Jersey: A study of the development of election machinery.* New Brunswick, NJ: Rutgers University Press.

McCloy, Joyce. 2005. *Operating cost comparison for different types of voting systems.* Greensboro, NC: North Carolina Coalition for Verified Voting. http://www.ncvoter.net/affordable.html (accessed February 20, 2007).

McCloy v. North Carolina State Board of Elections. 2005. Raleigh, NC: Wake County Superior Court.

Mebane, Walter R. Jr. 2004. The wrong man is president! Overvotes in the 2000 presidential election in Florida. *Perspectives in Politics* 2.

Mennite, Lori and David Callahan. 2003. Securing the vote: An analysis of election fraud. New York, NY: Demos.

Mercuri, Rebecca. 2002. *A better ballot box?* Philadelphia, PA: Notable Software. http://www.notablesoftware.com/Papers/1002evot.pdf (accessed February 20, 2007).

———. 2004. *Facts about voter verified paper ballots.* Philadelphia, PA: Notable Software. http://www.notablesoftware.com/Papers/VVPBFacts.pdf (accessed February 16, 2007).

Miller, John. 2007. Idaho mulls vote-by-mail measure. *Casper Star-Tribune*, February 20. http://www.casperstartribune.net/articles/2007/02/20/news/regional/88712d1493b56c3e8725728500268d18.txt (accessed February 20, 2007).

Miller, Ross. 2004. *Certification of voter-verified paper audit trail printer completed.* Carson City, NV: Office of the Secretary of State, July 16. http://209.85.165.104/search?q=cache:jjA9hjRpacsJ:www.sos.state.nv.us/press/071604.htm (accessed March 9, 2007).

Miller, William D. 1957. *Memphis during the progressive era, 1900-1917.* Memphis, TN: Memphis State University Press.

Miller, William D. 1964. *Mr. Crump of Memphis.* Baton Rouge, LA: Louisiana State University Press.

Milligan, Maurice M. 1948. *Missouri waltz: The inside story of the Pendergast machine by the man who smashed it.* New York: Charles Scribner's Sons.

Moore, James and Wayne Slater. 2003. *Bush's brain: How Karl Rove made George W. Bush presidential.* New York, NY: Wiley.

Moore, Justin. 2006. *Georgia per-county cost comparison.* http://www.cs.duke.edu/~justin/voting/ga-costs/ (accessed May 11, 2007).

Morris, Roy, Jr. 2003. *Fraud of the century: Rutherford B. Hayes, Samuel Tilden, and the stolen election of 1876.* New York: Simon and Schuster.

Multnomah County Elections Division. 2004. *Voting in Oregon - vote by mail.* Portland, OR. http://www.co.multnomah.or.us/dbcs/elections/election_information/voting_in_oregon.shtml (accessed February 16, 2007).

Myers, Gustavus. 1968. *The history of Tammany Hall.* New York, NY: Burt Franklin.

Myerson, Rosemarie. 2005. *Comparison of operating costs: Analysis of punch card and electronic voting machines in Sarasota County Florida and optical scanners in Manatee County Florida.* Bremerton, WA: Votersunite.org, February 8. http://votersunite.org/info/costcomparison.asp (accessed March 9, 2007).

National Association of Secretaries of State. 2004. *Fact sheet: The Help America Vote Act of 2002, H.R. 3295.* Washington, DC. http://www.nass.org/electioninfo/HAVA%20Fact%20Sheet2.pdf (accessed February 26, 2006).

National Conference of State Legislatures. 2004. *Recounts.* Washington, DC. http://www.ncsl.org/Programs/legismgt/elect/recounts.htm (accessed April 9, 2007).

Newkirk, M. Glenn. 2004. *U. S. public opinion toward voting technologies.* Raleigh, N.C.: InfoSENTRY Services, Inc.

New York Times. 2004. They said it couldn't be done, September 18. http://www.nytimes.com/2004/09/18/opinion/18sat2.html?ex=1173589200&en=2144b45dffdcc4ff&ei=5070 (accessed March 9, 2007).

New York Times Books. 2001. *Thirty-six days: The complete chronicle of the 2000 presidential election crisis by correspondents of the New York Times.*

New Yorkers for Verified Voting. Undated. *Cost comparison of voting equipment for New York State, touchscreen DRE with VVPB printer vs. precinct based optical scan +ballot marking device.* Mecklenburg, NY. http://www.nyvv.org/doc/CostComparisons.pdf (accessed February 21, 2007).

Noble, David F. 1977. *America by design: Science, technology, and the rise of corporate capitalism.* New York: Knopf.

North Carolina General Statutes § 163-165.7 and § 163-165.9.Nye, Joseph S., Phillip D. Zelikow, and David C. King, eds. 1997. *Why people don't trust government.* Cambridge, MA: Harvard University Press.

Oregon Elections Division. 2006. *Oregon Bulletin.* Salem, OR: Office of the Secretary of State, November 1. http://arcweb.sos.state.or.us/rules/1106_Bulletin/1106_ch165_bulletin.html (accessed March 5, 2007).

Palast, Greg. 2002. Ex-con game: How Florida's "felon" voter-purge was itself felonious. *Harper's*, March.

Parsons, William T. 1969. The bloody election of 1742. *Pennsylvania History* 36.

Patterson, Thomas E. 2002. *The vanishing voter: Public involvement in an age of uncertainty.* New York: Knopf.

People for the American Way. 2004. *Shattering the myth: An initial snapshot of voter disenfranchisement in the 2004 elections.* Washington, D.C.

Pildes, Richard H. 2002. Disputing elections. In *The longest night: Polemics and perspectives on election 2000*, by Arthur J. Jacobson and Michael Rosenfeld. Berkeley, CA: University of California Press.

Piven, Frances Fox and Richard A. Cloward. 2000. *Why Americans still don't vote and why politicians want it that way.* Boston: Beacon Press.

Rakove, Jack N., ed. 2001. *The unfinished election of 2000.* New York: Basic Books.

Redard, Thomas F. 1981. The election of 1844 in Louisiana: A new look at the ethno-cultural approach. *Louisiana History* 2.

Reynolds, John F. 1988. *Testing democracy: Electoral behavior and progressive reform in New Jersey, 1880-1910.* Chapel Hill, NC: University of North Carolina Press.

———. 1980. 'The silent dollar': Vote buying in New Jersey. *New Jersey History*, Fall-Winter.

Robertson, Gary D. 2005. Judge rejects challenge over N.C. voting equipment firms chosen. *newsobserver.com,* December 21. http://dwb.newsobserver.com/news/ncwire_news/story/ 2862233p-9318708c.html (accessed February 28, 2007).

Robinson, Lloyd. 2001. *The stolen election: Hayes versus Tilden, 1876.* New York, NY: Tom Doherty.

Rosenfeld, Michel. 2002. *Bush v. Gore:* Three strikes for the constitution, the court, and democracy, but there is always next season. In *The longest night: Polemics and perspectives on election* 2000, by Michael Rosenfeld and Arthur Jacobson. Berkeley, CA: University of California Press.

Roth, Susan. 1998. Disenfranchised by design: Voting systems and the election process. *Information Design Journal* 9: 1-8.

Rubin, Aviel D. 2006. *Brave new ballot.* New York, NY: Morgan Road Books.

Ryan, P.Y.A. 2006. *Computing science: Verified encrypted paper audit trails.* University of Newcastle upon Tyne Technical Report Series CS-TR-966*.* http://www.cs.ncl.ac.uk/ research/pubs/trs/papers/966.pdf (accessed February 20, 2007).

Sabato, Larry J. and Glenn R. Simpson. 1996. *Dirty little secrets: The persistence of corruption in American politics.* New York: Times Books.

Saltman, Roy G. 1988. *Accuracy, integrity, and security in computerized vote-tallying.* Gaithersburg, MD: National Board of Standards Special Publication 500-158.

———. 2006. *Independent verification: Essential action to ensure integrity in the voting process.* Gaithersburg, MD: National Institute of Standards and Technology.

San Bernardino County Registrar of Voters and Sequoia Voting Systems. 2004. *Joint report regarding the November 2, 2004 AVVPAT Sequoia VeriVote pilot project.* http://www.ss.ca.gov/elections/voting_systems/012005_1ai_v.pdf (accessed February 17, 2007).

Sarvis, Will. 2000. The irrepressible urge to manipulate election fraud in rural Missouri, 1940-1970. *Journal of the West* 39.

Schattschneider, E. E. 1950. *The semisovereign people: A realist's view of democracy in America.* New York: Holt, Rinehart and Winston.

———, ed. 1971. *The history of American presidential elections.* New York: Chelsea House.

Schneider, Mary Beth. 2007. Can mailbox become new ballot box? *Indianapolis Star*, February 12. http://www.indystar.com/apps/pbcs.dll/article?AID=/20070212/LOCAL190111/702120396/-1/ZONES04 (accessed February 20, 2007).

Science Applications International Corporation. 2003. *Risk assessment report: Diebold Accuvote-TS voting system and process.* Prepared for Maryland Department of Management and Budget.

Selker, Ted and Jon Goler. 2004. *Security vulnerabilities and problems with voter verified paper trails.* Pasadena, CA: California Institute of Technology and Massachusetts Institute of Technology, Voting Technology Project. http://www.vote.caltech.edu/media/documents/vtp_wp13.pdf (accessed May 2, 2007).

Sellers, Charles. 1966. *James K. Polk: Continentalist, 1843-1846.* Princeton, NJ: Princeton University Press.

Sequoia Voting Systems. 2004. *State of Nevada to utilize voter verifiable paper record printers throughout the state in 2004 primary and general election.* Oakland, CA. http://www.sequoiavote.com/article.php?id=56 (accessed February 20, 2006).

Sewell, Cynthia. 2007. Ada County will do away with punch-card ballots, move to optical scan system. *Idaho Statesman*, February 23. http://216.239.51.104/search?q=cache:IOspg0JdOWYJ:www.idahostatesman.com/102/story/72716.html (accessed March 12, 2007).

Smith, J. Allen. 1930. *The growth and decadence of constitutional government.* New York, NY: Henry Holt.

Smithsonian National Museum of American History. Undated. *Vote: The machinery of democracy.* Washington, DC. http://americanhistory.si.edu/vote/intro.html (accessed February 26, 2007).

Southwell, Priscilla L. 2004. Five years later: A re-assessment of Oregon's vote by mail electoral process. *PS: Political Science & Politics*, January: 89-93. http://www.apsanet.org/imgtest/FiveYearsLater-Southwell.pdf (accessed February 23, 2007).

Squires, James D. 1996. *The secrets of the Hopewell box: Stolen elections, southern politics, and a city's coming of age.* New York, NY: Times Books.

Steffens, Lincoln. 1905. Rhode Island: A state for sale. *McClure's Magazine* February.

———. 1964. Fraud and intimidation in the Florida election of 1876. *Florida Historical Quarterly*, April.

Stein, Ronert M., Jan Leighley and Christopher Owens. 2005. *Who votes, who doesn't, why, and what can be done?* Washington, DC: Federal Commission on Election Reform. http://www.american.edu/ia/cfer/0630test/stein.pdf (accessed March 12, 2007).

Stewart, Warren. 2007. Written testimony of Warren Stewart, Policy Director, VoteTrustUSA before the Committee on House Administration, Elections Subcommittee, U.S. House of Representatives. https://www.verifiedvotingfoundation.org/downloads/Stewart%20Testimony-4.pdf (accessed May 11, 2007).

Summers, Mark Wahlgren. 1987. *The plundering generation: Corruption and the crisis of the union 1849-1861.* New York, NY: Oxford University Press.

———. 1993. *The era of good stealings.* New York, NY: Oxford University Press.

———. 2000. *Rum, Romanism, & Rebellion: The Making of a President, 1884.* Chapel Hill, NC: University of North Carolina Press.

———. 2004. *Party games: Getting, keeping, and using power in gilded age politics.* Chapel Hill, NC: University of North Carolina Press.

Tapper, Jake. 2001. *Down and dirty: The plot to steal the presidency.* New York: Little, Brown.

Teixeira, Ruy A. 1992. *The disappearing American voter.* Washington, DC: Brookings Institution.

Tennessee Division of Elections. 2006. *Elections - absentee voting.* Nashville, TN: Department of State. http://tennessee.gov/sos/election/absentee.htm (accessed February 23, 2007).

Tennessee Division of Elections. 2006. *Statistical analysis of voter turnout for the November 7, 2006 election.* Nashville, TN: Department of State. http://www.state.tn.us/sos/election/data/turnout/2006-11.pdf (accessed March 12, 2007).

Testi, Arnaldo. 2001. The tribulations of an old democracy. *Journal of American History* 88.

Thompson, Dennis F. 2002. *Just elections: Creating a fair electoral process in the United States.* Chicago, IL: University of Chicago Press.

Tokaji, Daniel P. 2004. *The paperless chase: Electronic voting and democratic values.* Columbus, OH: The Ohio State University Moritz College of Law, Center for Law, Policy, and Social Science.

Toobin, Jeffrey. 2001. *Too close to call: The thirty-six day battle to decide the 2000 election.* New York, NY: Random House.

Uggen, Christopher and Jeff Manza. 2002. Democratic contraction? The political consequences of felon disenfranchisement in the United States. *American Sociological Review* 67: 777-803.

U.S. Election Assistance Commission. 2004. *Improving the Usability and Accessibility of Voting Systems and Products.* Washington, DC.

———. 2006. *Best practices in election administration.* Washington, DC.

———. Undated. *About the EAC.* Washington, DC. http://www.eac.gov/about.asp (accessed February 21, 2007).

———. Undated. *Best practices tool kit: Optical scan voting systems.* Washington, DC. http://www.eac.gov/bp/index1.asp?view=print&format=textonly (accessed February 23, 2007).

———. Undated. *Quick start management guide for voting system security.* Washington, DC. http://www.eac.gov/docs/QA_EDIT_VotSysSecurity2.pdf (accessed February 21, 2007).

U. S. Government Accountability Office. 2005. *Elections: Federal efforts to improve security and reliability of electronic voting systems.* Washington, DC.

U. S. Government Accountability Office. 2006. *Elections: The nation's evolving election system as reflected in the November 2004 general election.* Washington, DC.

U. S. Government Accountability Office. 2006. *Elections: 2005 survey of state election officials.* Washington, DC.

U.S. House of Representatives, Democratic Investigative Staff, House Committee on the Judiciary. 2001. *How to make over one million votes disappear: Electoral sleight of hand in the 2000 presidential election.*

United States of America v. New York State Board of Elections. 2006. Civil Action number 06-CV-0263. Syracuse, NY: United States District Court for the Northern District of New York.

Verified Voting Foundation. Undated. *Are voter-verified paper ballots cost-effective?* Wilmington, DE. http://www.verifiedvoting.org/index.php (accessed February 21, 2007).

———. Undated. *Verified voting: Mandatory manual audits of voter-verified paper records.* Wilmington,DE: http://www.verifiedvoting.org/?printsafe=1 (accessed February 16, 2007).

VotersUnite.org. 2006. *Diebold in the news-A partial list of documented failures.* Bremerton, WA. http://www.votersunite.org/info/Dieboldinthenews.pdf (accessed February 21, 2007).

Wagner, David. 2007. Written Testimony of David Wagner, Ph.D., Computer Science Division, University of California, Berkeley, before the Committee on House Administration, Elections

Subcommittee, U.S. House of Representatives, March 15, 2007. http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf (accessed August 28, 2007)

Wallach, Dan. 2006. *Report in the Colorado Direct Recording Electronic ("DRE") voting systems case, Conroy v. Colorado Secretary of State Ginnette Dennis*. http://accurate-voting.org/wp-content/uploads/2006/09/dwallach-redacted-new.pdf (accessed November 16, 2007).

Walker, Robert L. Undated. *Voting System Testing.* Annapolis, MD: Maryland State Board of Elections. http://www.elections.state.md.us/voting_system/testing.html (accessed May 16, 2007).

Washburn, John. 2006. *A guideline for creating a deck of test ballots.* Germantown, WI: Washburn Research. http://www.washburnresearch.org/archive/TestingGuidelines/GuidelinesForCreatingTestBallots.pdf (accessed February 28, 2007).

Washington Office of the Secretary of State. 2006a. *Elections: Frequently asked questions on voting by mail.* Olympia, WA. http://www.secstate.wa.gov/elections/faq_vote_by_mail.aspx (accessed February 20, 2007).

———. 2006b. *Elections: Voting by absentee ballot.* Olympia, WA. http://www.secstate.wa.gov/elections/register_absentee.aspx (accessed February 23, 2007).

Watson, Robert P. 2004. The state of elections: People, politics, and problems. In *Counting Votes: Lessons from the 2000 Presidential Election in* Florida, ed. Robert P. Watson. Gainesville, FL: University Press of Florida.

White, Theodore H. 1961. *The making of the president, 1960.* New York, NY: Atheneum.

Williams, Walter. 2003. *Reaganism and the death of representative democracy.* Washington, DC: Georgetown University Press.

Wills, Garry. 1999. *A necessary evil: A history of American distrust of government.* New York: Simon and Schuster.

Wise, Charles. 2001. Election administration in crisis: An early look at lessons from Bush versus Gore. *Public Administration Review* 61.

Woodruff, Clinton Rogers. 1901. Election methods and reforms in Philadelphia. *Annals of the American Academy of Political and Social Science*, March.

Wright, George C. 1984. The billy club and the ballot: Police intimidation of blacks in Louisville, Kentucky, 1880-1930. *Southern Studies* 23.

Zogby International. 2006. *Americans concerned about election transparency and security.* Utica, NY. http://www.zogby.com/News/ReadNews.dbm?ID=1163 (accessed February 22, 2007).

TACIR Members

Representative Randy Rinks, Chairman
Mayor Tom Rowland, Vice Chairman
Harry A. Green, Executive Director

Legislative

Senator Rosalind Kurita
Senator James Kyle
Senator Mark Norris
Senator Jim Tracy
Representative Jason Mumpower
Representative Gary Odom
Representative Randy Rinks
Representative Larry Turner

Statutory

Representative Craig Fitzhugh, Chairman, Finance Ways & Means Committee
Senator Randy McNally Chairman, Finance Ways & Means Committee
Comptroller John Morgan

Executive Branch

Paula Davis, Department of Economic & Community Development
Drew Kim, Governor's Office

Municipal

Tommy Bragg, Mayor of Murfreesboro
Sharon Goldsworthy, Mayor of Germantown
Bob Kirk, Alderman, City of Dyersburg
Tom Rowland, Mayor of Cleveland

County

Rogers Anderson, Williamson County Mayor
Kim Blaylock, Putnam County Executive
Jeff Huffman, Tipton County Executive
R.J. Hank Thompson, Sumner County Executive

Other Local Officials

Brent Greer, Tennessee Development District Association
Charles Cardwell, County Officials Association of Tennessee

Private Citizens

John Johnson, Morristown
Tommy Schumpert, Knoxville

Commissioner Emeritus

Senator Douglas Henry