

ELECTION REFORM



MALFUNCTION AND MALFEASANCE **A REPORT ON THE ELECTRONIC VOTING MACHINE DEBACLE**



COMMON CAUSE

Holding Power Accountable

Acknowledgements

The Common Cause team responsible for this report consisted of: Matt Shaffer, chief researcher; Barbara Burt and Susannah Goodman, writers; Mary Boyle, Edwin Davis, and Jenny Flanagan, readers; and Stephen Steigleder, research assistant.

The following people contributed ideas, information, or comments to this report: Doug Chapin, Rich Garella, John Gideon, Eleanor LeCain, John McCarthy, Toby Moore, Michelle Mulder, Lawrence Norden, Spencer Overton, Lawrence Rockefeller, Warren Stewart, and Tova Wang. We are grateful for their insights but all mistakes are ours alone. Please note that our acknowledgement of their contributions does not necessarily mean they endorse our recommendations.

We are especially indebted to Pam Smith of Verified Voting. She and her colleagues provided the information that made the charts possible. Pam also generously shared her vast knowledge of this issue to help us make sense of the current voting machine debacle.



A special Election Reform report prepared by:
Common Cause
1133 19th Street NW, 9th Floor
Washington, D.C. 20036
202.833.1200

www.commoncause.org

Contents

Executive Summary	3
Introduction	5
I. Political Forces That Led to the Popularity of DREs	5
II. The Weaknesses of DRE Systems	6
Studies Show That DREs Are Vulnerable to Tampering and Failure	7
Johns Hopkins University Information Security Institute Technical Report	7
2005 GAO Study on Election Machine Security and Reliability	8
Carter Baker Commission on Federal Election Reform	8
May 2006 Black Box Voting Report on Critical Security Issues with the Diebold TSx	9
Actual Machine Failures	10
Texas	10
North Carolina	11
Pennsylvania	11
Florida	11
Virginia	12
New Mexico	13
III. Citizens and State Legislatures Take Action to Correct DRE-Related Problems	13
National Action	13
State Action	14
Nevada	14
California	15
Ohio	15
The Current Status of State Legislation	15
Rethinking the Bias Toward DREs	16
IV. Citizens and Reform Groups Take Legal Action to Stop States from Buying DRE Systems	16
Chart A Status of State Voting Systems	18
Chart B State-by-State Voter Risk Assessment	19
Chart C High-Risk States That Allow No-Excuse Absentee Voting	20
V. Recommendations	21
VI. Endnotes	23

ELECTION REFORM

malfunction and malfeasance

A Report on the Electronic Voting Machine Debacle

Common Cause, a nonpartisan, nonprofit organization committed to honest, open and accountable government, studied available information on voting machine technology and concluded that the push to use direct recording electronic (DRE) voting machines was misguided, has resulted in serious security and reliability concerns, and should be reversed. Common Cause concludes that the only way to ensure accurate election results is to require all voting systems to produce a voter verified paper ballot—either marked by the voter or printed by an electronic voting machine or a ballot-marking machine and approved by the voter—and a statistically meaningful and transparent audit process.

Executive Summary

This report surveys four major studies that reviewed DRE voting machine security and reliability. Two of the reports involved extensive review of more than 80 academic, technical, and industry reports on DREs. Each report concluded that DRE machines to be vulnerable to malfunction and also to tampering in which a computer-savvy hacker with minimal access to the machine could introduce malicious code to the DRE software and change the results of an election. Such manipulation could be undetectable. In machines equipped with a modem, it could even be done from a remote location.

Furthermore, there have been at least seven reported occasions since 2002 in which electronic voting machines added or removed votes in real elections, calling into question the final results of a race. For example, this spring, as states across the country conducted primary elections, a programming error caused a DRE in Tarrant County, Texas, to record an additional 100,000 votes that were never actually cast. The election outcome is being challenged by a candidate who lost by 6,000 votes.

Despite the security problems and serious malfunctions, in November DRE machines will be used in 37 states, with 39 percent of voters expected to vote on them. In many of these states, there are no adequate safeguards in place. State law either does not require the voting system to produce a voter-verified paper ballot or does not require a statistically meaningful and transparent audit process. These states are at risk of compromised elections due to DRE malfunction or tampering.

Because electronic voting machines do not produce an independently verifiable paper voting record, there is no good record that can be used for an audit or a recount. Although some electronic voting machines do keep paper records of the complete ballot image, not every machine does. And unfortunately, if the machine malfunctions or the computer code has been the subject of tampering, this record is no longer reliable.

This report includes a chart detailing the status of each state, along with a chart detailing the level of risk for voters in each state, and chart showing which medium and high risk states allow no-excuse absentee voting.

To address these problems, Common Cause makes eight recommendations:

- Congress should immediately pass HR 550, “The Voter Confidence and Increased Accessibility Act of 2005.”
- States should pass laws or adopt regulations requiring all voting systems to produce a voter verifiable paper ballot and mandate that at least a random two percent of voting jurisdictions conduct public audits of their voting systems.
- Election officials should take necessary steps to safeguard machines prior to Election Day.
- State election officials should, wherever possible, immediately retrofit DREs with printing systems to produce a voter verifiable paper ballot, and use those ballots in audits.
- In the instance where DREs cannot be retrofitted, Common Cause recommends that state election officials decertify those DREs that cannot provide a paper record and turn to other voting systems such as optical scan machines for the November elections.
- Congress and states should make emergency funds available for purchase or lease of more secure, auditable machines.
- Voters should be encouraged to vote on paper whenever possible. If facing the prospect of voting on paperless DREs in November, they should advocate for change with local election officials well before the election. If that does not work, where possible, voters should vote by absentee ballot.
- Regardless of the voting equipment in a jurisdiction, citizens should vote. While there is a chance that a vote won’t be counted if cast on a paperless DRE, not voting at all will assure that it is not.

Regardless of the voting equipment in a jurisdiction, citizens should vote. While there is a chance that a vote won’t be counted if cast on a paperless DRE, not voting at all will assure that it is not.



Introduction

With five months to go before the critical 2006 mid-term elections, serious questions about the reliability and security of paperless electronic voting machines known as Direct Recording Electronic (DRE) devices continue to be raised nationwide. Major security concerns have been documented in at least four major reports, and a number of states that held primary elections this spring saw problems with DREs. Yet nearly 40 percent of voters are expected to cast ballots on DREs in November, and Congress continues to ignore the problems.

This report reviews the political circumstances that led to the popularity of DREs, details the security and reliability problems posed by DREs and presents information showing which states use DREs and which ones are at greatest risk of having elections compromised due to problems with DREs. It also lays out recommendations for citizens who will have to use DREs to vote on Election Day.

I. Political Forces that Led to the Popularity of Electronic Voting Machines

The Help America Vote Act (HAVA) was passed in 2002 to rectify some of the problems in our election system exposed during the 2000 presidential elections. Plagued by the memory of election officials haggling over hanging chad, Congress included requirements calling for technological advances in election system machinery. Voting rights activists saw an opportunity to push for improvements in voting machines that would allow disabled voters to vote independently and privately; advocates for non-English speakers saw a chance to make it easier to offer ballots in many languages. The needs of both populations became a factor in the design of the new equipment.

Consequently, HAVA required that:

1) All voting systems used in federal elections provide people with disabilities, including the blind or visually impaired, the same access to voting as other voters, “through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place.” properly equipped voting system in each polling place.”¹

2) All punch card and lever machine systems be completely replaced with machines accessible to the disabled.

This report reviews the political circumstances that led to the popularity of DREs, details the security and reliability problems posed by DREs and presents information showing which states use DREs and which ones are at greatest risk of having elections compromised due to problems with DREs. It also lays out recommendations for citizens who will have to use DREs to vote on Election Day.

Congress also provided federal funding through HAVA for states to replace their voting systems with new systems that met these new requirements. Also, HAVA set a deadline for all the new voting system requirements to be in place. This deadline was to be the first election involving federal candidates in 2006—in other words, the primary elections of this spring.

Because punch card and lever voting machines were used in many precincts, jurisdictions across the country were faced with the task of choosing entirely new voting systems. The DRE became one of the most popular options for several reasons, including the fact that language in HAVA encouraged the purchase of these machines, federal funding was available to buy them and looming deadlines demanded fast decisions.

Election officials' attraction to DREs was understandable. The voting machine manufacturers and other advocates of the systems claimed that they could tabulate votes faster, were easy to use and could be easily adjusted to operate in different languages. Perhaps most persuasive was the claim by DRE manufacturers that DREs meet the needs of disabled voters.^{2*}

As a result of the perception that DREs could best meet the requirements of HAVA, DRE use in counties across the country has more than tripled, rising from 320 counties in November 2000 to an expected 1,050 counties this November. In 2006, 39 percent of registered voters are expected to use DRE voting machines. That is only slightly less than the 41 percent of voters expected to use the most popular type of voting equipment, the optical scan machine.³

II. The Weaknesses of DRE Systems

Unfortunately, despite the stellar sales pitch, DREs are highly vulnerable to machine malfunction and human manipulation. The two largest concerns are their lack of transparency and the fact that they do not produce a back-up system that can allow for a recount.

When a citizen casts a vote on an electronic voting machine, there is no way for that person to ensure that the vote was recorded correctly. Software code inside the machine can be programmed to display the correct vote on the voting screen, but the vote in fact could be recorded incorrectly. In other words, a citizen could pick candidate John Smith for president, and the screen could show that the citizen picked John Smith, but the computer could be programmed to record the vote for Bill Blue.

* **Common Cause**

believes that every effort should be made to enable disabled voters to cast their votes privately. However, it is clear that no one machine will be able to solve all the varied problems disabled voters face. More likely, a menu of add-on features will need to be used to make voting truly accessible to all. But paramount in our thinking about solving problems of physical access should be consideration of not only privacy but also verifiability. The ballots of disabled voters deserve the same level of security as those of other voters.



Because electronic voting machines do not produce an independently verifiable paper voting record, there is no good record that can be used for an audit or a recount. Although some electronic voting machines do keep paper records of the complete ballot image, not every machine does. And unfortunately, if the machine malfunctions or the computer code has been the subject of tampering, this record is no longer reliable.

In other words, there is no way to recount the vote tallies recorded by a DRE machine, nor is there any way to retrieve previously recorded votes if the data is erased or corrupted. Election officials must place their trust into the design and performance of the machine, despite the fact that the software is trade-secret protected and cannot be inspected, even by election officials in most cases.⁴ This lack of transparency and the lack of a back-up system makes these machines inappropriate for use in elections unless appropriate safeguards are put in place.

Studies Show That DREs are Vulnerable to Tampering and Failure

A number of studies and policy papers have concluded that DREs are vulnerable to tampering. Four of the more prominent studies are reviewed here.

Johns Hopkins University Information Security Institute Technical Report

In 2003, computer science professors from Johns Hopkins University, led by Dr. Avi Rubin, released one of the first widely circulated reports analyzing the security standards of a DRE system. In their report, "Analysis of an Electronic Voting System," which reviewed Diebold's AccuVote-TS systems, they found a string of vulnerabilities making the machines susceptible to tampering. For example, to operate the Diebold machines on Election Day, poll workers provide voters with "smartcards," which are required to be entered into the machine to record a vote. The study found that it would be relatively easy for somebody to program their own "smartcard" and manipulate data. They also found that someone could intercept machines' transfer information electronically and discovered weaknesses in the programming code. Dr. Rubin stated that he would have flunked a first-year student who turned in a program with such weak code.⁵

Because electronic voting machines do not produce an independently verifiable paper voting record, there is no good record that can be used for an audit or a recount. Although some electronic voting machines do keep paper records of the complete ballot image, not every machine does. And unfortunately, if the machine malfunctions or the computer code has been the subject of tampering, this record is no longer reliable.

The Johns Hopkins study sparked a flurry of concern. The state of Maryland commissioned RABA Technologies, a Columbia, MD based software system and engineering firm to examine and critique the study. In its review, RABA Technologies called for a “pervasive rewrite” of Diebold’s code.⁶ The study was also reviewed in a report entitled “Risk Assessment Report Diebold Accuvote-TS Voting System and Processes” prepared by Science Applications International Corporation, which also identified problems with the Accuvote-TS source code.⁷

2005 GAO Study on Election Machine Security and Reliability

In 2005, the Government Accountability Office (GAO) released an extensive report assessing the significant security and reliability concerns that have been identified with electronic voting systems. The report, entitled “Federal efforts to improve security and reliability of electronic voting systems are under way, but key activities need to be completed,” surveyed over 80 studies and research reports related to the security of electronic voting systems and focused on systems associated with vote casting and counting. The report noted that these studies listed a number of potential security flaws including weak security controls, system design flaws, inadequate system version control, inadequate security testing, incorrect system configuration, and poor security management.

In characterizing some of the studies, the GAO noted that “studies found (1) some electronic voting systems did not encrypt cast ballots or system audit logs, and it was possible to alter both without being detected; (2) it was possible to alter the files that define how a ballot looks and works so that the votes for one candidate could be recorded for a different candidate; and (3) vendors installed uncertified versions of voting system software at the local level.”⁸

In their conclusion, the authors of the report noted that their review “pointed to a situation in which vendors may not be uniformly building security and reliability into their voting systems, and election officials may not always rigorously ensure the security and reliability of their systems when they acquire, test, operate and manage them.”⁹

Carter Baker Commission on Federal Election Reform

In 2005, the Commission on Federal Election Reform was established to research the state of elections in the United States and offer recommendations for improvement. The bipartisan commission was led by former Democratic President Jimmy Carter and former Republican Secretary of State James Baker. In September 2005, the commission released its broad set of reform proposals covering a wide array of election issues. Key among them were the issues presented by voting technology.

In their conclusion, the authors of the report noted that their review “pointed to a situation in which vendors may not be uniformly building security and reliability into their voting systems, and election officials may not always rigorously ensure the security and reliability of their systems when they acquire, test, operate and manage them.”



The commissioners surveyed existing reports, academic studies, and other material to formulate their recommendations for DRE technology. They concluded that the benefits of DREs were offset by a lack of transparency and noted that DREs do not allow voters to check if their ballot is recorded correctly and that some DREs have no capacity for an independent recount. In their final report, the commissioners recommended that Congress pass legislation requiring all voting systems to produce a voter verified paper record and that states adopt formal auditing procedures to reconcile any disparity between the electronic ballot tally and the paper ballot tally. The text of the recommendations follows:

Congress should pass a law requiring that all voting machines be equipped with a voter-verifiable paper audit trail and, consistent with HAVA, be fully accessible to voters with disabilities. This is especially important for direct recording electronic (DRE) machines for four reasons: (a) to increase citizens' confidence that their vote will be counted accurately, (b) to allow for a recount, (c) to provide a backup in cases of loss of votes due to computer malfunction, and (d) to test-through random selection of machines – whether the paper result is the same as the electronic result. Federal funds should be appropriated to the EAC to transfer to the states to implement this law. While paper trails and ballots currently provide the only means to meet the Commission's recommended standards for transparency, new technologies may do so more effectively in the future. The Commission therefore urges research and development of new technologies to enhance transparency, security, and auditability of voting systems.

States should adopt unambiguous procedures to reconcile any disparity between the electronic ballot tally and the paper ballot tally. The Commission strongly recommends that states determine well in advance of elections which will be the ballot of record.¹⁰

States should adopt unambiguous procedures to reconcile any disparity between the electronic ballot tally and the paper ballot tally. The Commission strongly recommends that states determine well in advance of elections which will be the ballot of record.

May 2006 Black Box Voting Report on Critical Security Issues with the Diebold TSX

In May 2006, Finnish computer security expert Harri Hursti working with the organization BlackBoxVoting.org released a report documenting several security issues with the Diebold electronic voting terminals TSx and TS6. According to the report, “the security threats seem to enable a malicious person to compromise the equipment even years before actually using the exploit, possibly leaving the voting terminal incurably compromised.”¹¹ In other words, a computer hacker, doubling as a poll worker, would only need a few seconds of physical access to the machines to introduce a virus to the software by putting a memory card inside of the machine. Because the memory cards are transferred from one machine to another, this could cause the machines to fail or to simply change the vote outcome by switching votes.¹²

Computer scientists who work in the field reacted with shock at the extent of the vulnerability. Michael Shamos, a computer science professor at Carnegie Mellon University and long-time proponent of electronic voting machines, said: “It’s the most severe security flaw ever discovered in a voting system.”¹³ Dr. Rubin, the computer science professor at Johns Hopkins and co-author of the previously mentioned study exposing technical flaws in a Diebold voting machine, said he feared that the latest security problem could be serious enough to cause an Election Day “meltdown” that could put precincts of machines out of action.¹⁴ “It is like the nuclear bomb for e-voting systems,” Dr. Rubin said. “It really makes the security flaw we found in [in prior years] look trivial.”¹⁵

Actual Machine Failures

Problems with DREs are not theoretical. There are a number of instances where electronic voting machines have added or removed votes in real elections, throwing the outcome of the election into question. Below are just a few examples where voting machine failures were so egregious that they were detected.

Texas

During this year’s Texas primaries in March, a programming error caused voting machines in Tarrant County to record an additional 100,000 votes that were never actually cast. Election officials were shocked when the initial tallies showed that 158,000 voters came to the polls, a number that would have shattered the previous primary turnout record and more than doubled the turnout of 76,000 in 2002.

A programming mistake in the machine’s software by a company responsible for both hardware and software, Hart Intercivic, boosted vote totals far beyond the 58,000 votes that were actually cast. The company said that the error boosted the totals equally for every candidate and that the election outcomes were not affected.¹⁶

Hart Intercivic accepted full responsibility for the error, but some people were not satisfied with the outcome. Justice Steve Smith, a candidate for the Texas State Supreme Court, filed a formal challenge to the election results, which showed he lost his bid by 6,000 votes. In a statement to the Fort Worth Star Telegram, he wrote, “We have good reason to believe that the vote total is incorrect, and we believe that the election must not be finally decided until all the votes are correctly counted.”¹⁷

Dr. Rubin, the computer science professor

at Johns Hopkins and co-author of the previously mentioned study exposing technical flaws in a Diebold voting machine, said he feared that the latest security problem could be serious enough to cause an Election Day “meltdown” that could put precincts of machines out of action.



North Carolina

In November 2004, 4,438 votes were lost by an electronic voting machine in Carteret County, North Carolina, leaving the race for state agricultural commissioner in limbo for months. On Election Night, 3.3 million ballots were cast and Republican Steve Troxler led Democrat Britt Cobb by 2,287 votes. With almost twice that amount of votes permanently erased, a contentious legal battle ensued that only ended three months later when Cobb decided to concede the election.¹⁸

The source of the error was the Unilect Patriot, a touchscreen voting machine. Like most DREs, it had no backup system. In 2005, the Cartaret Board of Elections unanimously voted to replace the Unilect machines. “You cannot believe how much damage that has done to the question of voter confidence in the county,” said Ed Pond, the county elections board chairman.¹⁹

Pennsylvania

In April 2005, Pennsylvania decertified the UniLect Patriot electronic voting machine after concluding that defects in the system were responsible for more than 10,000 uncounted votes in three different counties in November 2004. When the state re-examined the machines after the elections, it found that the machines often failed to register votes after the voter pressed the screen to make his or her selection. The machines were also prone to freezing up during use.²⁰

In a separate incident in Berks County, Pennsylvania, involving voting machines manufactured by Danaher Controls, 111 votes were lost when the cartridges used to record votes were accidentally programmed as training cartridges during the May 2005 primary election.²¹ Election results showed that three races were decided by less than 111 votes. After much controversy, the Berks County Election Board ultimately voted against having a re-vote.²²

Florida

During a special election on the issue of slot machines, Miami-Dade County’s new Elections Systems & Software (ES&S) iVotronic electronic voting machines produced more than 1,200 undervotes, despite the fact that there was only one issue on the ballot. Undervotes are counted ballots that contain no votes for candidates or issues, and a high number of them typically indicates a problem with the machine.

In April 2005, Pennsylvania decertified the UniLect Patriot electronic voting machine after concluding that defects in the system were responsible for more than 10,000 uncounted votes in three different counties in November 2004.

The county already had a history of election troubles. It was one of the counties scrutinized during the 2000 presidential election, and had continued problems in 2002 and 2004. Approximately one-third of the miscast votes were blamed on improper coding of cartridges by the county staff. Similar discrepancies were found in five other elections in the prior twelve months, though officials say that the amount of undervotes couldn't have affected the outcome of any of those elections.²³

To explain the other undervotes, Elections Supervisor Constance Kaplan said that many voters did not understand the ballot question and left in frustration before casting votes. ES&S and Kaplan blamed each other for the coding errors. Kaplan said that an ES&S program manager should have caught the error. According to ES&S officials, "the primary responsibility for this particular aspect for the election lies with the county." County official publicly criticized Kaplan and she was soon forced to resign.²⁴ In the meantime, the current elections supervisor Lester Sola has since recommended that the county replace their \$25 million system for an optical scanning system, citing the decline in voter confidence and increasing costs associated with the current DRE system.²⁵

Virginia

The failure of ten electronic voting machines cast doubt on the results of a local election in Fairfax County, Virginia during November 2003. Voters claimed that the machines failed to register their votes for incumbent school board member Rita S. Thompson (R), who lost by 1,662 votes. When testing one of the questionable machines, elections officials observed that it appeared to subtract a vote from Thompson for about one out of every 100 attempts to vote for her.

According to reports from multiple voters, the machine would initially display an "x" next to Thompson's name after she was selected, but the "x" would disappear seconds later. Another voter said that it took him four or five tries to register his vote for Thompson.²⁶

It was impossible to determine whether lost votes were intended for Thompson or whether other candidates also lost votes, and the questionable elections results were certified without any adjustment.²⁷

Voters claimed that the machines failed to register their votes for incumbent School Board member Rita S. Thompson (R), who lost by 1,662 votes. When testing one of the questionable machines, elections officials observed that it appeared to subtract a vote from Thompson for about one out of every 100 attempts.



New Mexico

A week before the 2004 election, Bernalillo County Clerk Mary Herrera admitted recurrent problems with vote recording software and that phantom votes had been recorded in three separate elections. She said that, in one instance, a candidate received an additional 4,000 votes that did not exist. However, Herrera claimed that the phantom votes were found before they were added to the final tally.²⁸

In 2002, only three-quarters of ballots cast in Bernalillo County's early voting period were initially tallied by Sequoia's DRE voting machines. According to Sequoia, 12,000 votes were omitted because "an employee had missed a step in the tallying process." Apparently, the software program used to report election results did not have the capacity to handle the data.²⁹ The company developed a "patch" to expand the program's capacity, but it wasn't passed along to its technician in Bernalillo County. The mistake, originally noticed by a partisan attorney during post-election analysis, delayed certification of the election results while the Board of Commissioners corrected the results.³⁰

On June 12, 2006, at their annual convention, the League of Women Voters passed a resolution in support of voter verified paper records and mandatory random manual audits of voting systems nationwide.

III. Citizens and State Legislatures Take Action to Correct DRE-Related Problems

As reports continue to reveal the potential vulnerabilities of DREs, concerned citizens in states and counties that have already bought or are in the process of purchasing these machines argue that if DREs must be used, then they should be outfitted with the capacity to produce a voter-verified paper ballot to confirm tallies produced internally by the machines. On June 12, 2006, at their annual convention, the League of Women Voters passed a resolution in support of voter verified paper records and mandatory random manual audits of voting systems nationwide. Other national groups such as Common Cause, Verified Voting, and VoteTrustUSA have been working with citizens, election officials, and elected representatives to pass corrective legislation at the state and federal level.

National Action

In May 2003, Representative Rush Holt (D-NJ) introduced federal legislation calling for a voter-verified paper record for every vote cast, as well as mandated audits comparing the paper records with machine totals.³¹ The bill was introduced into the House Administration Committee, which at the time was led by Representative Bob Ney (R-OH), a HAVA sponsor. Ney refused to bring the bill before the committee for discussion and a vote.³²

During the 109th Congress, Representative Holt improved and reintroduced the legislation, calling it the “The Voter Confidence and Increased Accessibility of 2005” (HR 550). The bill is widely supported by citizen advocacy groups and currently is co-sponsored by 191 members of the House of Representatives from both parties.³³ Representative Ney stepped down from his committee chairmanship due to his ties with the indicted lobbyist Jack Abramoff. Representative Vernon Ehlers (R-MI) has been appointed as the new chairman of the House Administration Committee.³⁴ Like Holt, Ehlers is a former scientist conversant with technological issues.³⁵ Recently, Ehlers has signaled his intention to hold a hearing on H.R. 550 and other election issues “sometime in the fall before the election.”³⁶

Also, in the Senate, Senator John Ensign (R-NV) introduced the Voting Integrity and Verification Act, (S. 17), which also calls for every voting system to produce a voter verifiable paper record, although this legislation does not mandate audits comparing paper records to machine totals.

State Action

By 2004, three states had passed laws or enacted regulations requiring that DREs be equipped with a voter verified paper ballot. Ohio and California’s laws required that their machines be equipped after 2004, while Nevada’s secretary of state, who had the responsibility for purchasing all voting systems for the entire state, took the additional step of requiring that all new machines to be used for the 2004 general election be equipped with printing devices to produce a paper trail.

Nevada

In December 2003, Nevada became the first state to mandate that voter-verified printouts be used with DREs when Secretary of State Dean Heller required that printers be used with Sequoia voting machines in 2004. Heller chose Sequoia’s machines over Diebold’s after he asked the state’s Gaming Control Board, which is responsible for inspecting slot machines used in the state’s casinos, to look at the two systems. The gaming board concluded that the Diebold machines “represented a legitimate threat to the integrity of the election process.”³⁷

Despite having confidence that Nevada chose the more secure voting system, Heller announced that all of the new machines would be outfitted with printing devices and that existing voting machines would be outfitted with similar printers. “By requiring a [voter verified receipt] printer to be a component of each DRE machine, voters will be confident their choices are being recorded accurately,” Heller said.³⁸

Despite having

confidence that Nevada chose the more secure voting system, Heller announced that all of the new machines would be outfitted with printing devices and that existing voting machines would be outfitted with similar printers.



California

In April 2004, Kevin Shelley, then California's secretary of state, announced his intention to have all voting machines used in his state produce a paper trail. He also announced a ban of the use of all Diebold TSx systems and temporarily decertified all other DRE systems until "security measures are met." In addition, Shelley asserted, "Diebold's persistent and aggressive marketing led to installation in a number of counties of touchscreen systems that were neither tested, qualified at the federal level, nor certified at the state level--and that Diebold then lied about it to state officials."³⁹ Shelley eventually recertified other machines on a county-by-county basis as they met specific security conditions, but 2004 was the last year that the machines operated without a paper printer. In September, Governor Arnold Schwarzenegger signed a law that would require all DRE machines to be equipped with a voter verified paper printout in 2005.⁴⁰

Unfortunately, Shelley's replacement, Secretary of State Bruce MacPherson, reversed Shelley's ban on Diebold TSx machines. There is currently a lawsuit in California to challenge the secretary of state's certification of these previously banned machines.⁴¹

Ohio

Ohio passed a law in May 2004 that would require DRE voting machines to be equipped with a voter verified paper ballots by 2006.

In early 2004, Ohio Secretary of State Ken Blackwell gave approval for Ohio counties to purchase one of three brands of touch-screen voting machines: Diebold, ES&S and Hart Intercivic. Five months before the general election, however, Blackwell halted the deployment of the Diebold machines because of security concerns. This meant that the counties originally scheduled to use the touch screen machines had to rely predominantly on the unreliable punch cards that most Ohio counties had used in the past. Ohio's use of punch cards became the subject of a lawsuit against the state by the ACLU, which claimed that the use of punch cards disproportionately harms low-income and minority precincts because their ballots are more likely to be thrown out.

The Current Status of State Legislation

After the 2004 election, a number of state legislatures passed laws that required their voting systems to produce a voter verifiable paper record. Additionally, a number of secretaries of state and governors took up the issue and either by supporting statewide legislation or by regulation have required their voting systems to produce voter verifiable paper records.

Ohio's use of punch cards became the source of a lawsuit against the state by ACLU, who claimed that the use of punch cards disproportionately harms low-income and minority precincts because their ballots are more likely to be thrown out.

For example, in January 2006, New Mexico Governor Bill Richardson asked the legislature to pass a law retiring all electronic paperless voting machines from use in the state's polling places, and requiring that optical scan machines be installed instead.⁴² The bill passed and was signed into law in March.⁴³

As of this printing, 27 states have enacted laws or established administrative rules requiring voting systems to produce voter-verifiable paper records. Fifteen of those states require an audit of the voting system to ensure accuracy (see chart A on page 20).

Rethinking the Bias Toward DREs

Among the first to purchase and implement DRE machines, states including Florida, Georgia and Maryland are now actively considering changing voting systems, reflecting a sea-change in the confidence citizens have in these machines.

When Georgia purchased its \$54 million DRE voting system, election officials were proud to be among the first to update their machines in the wake of the 2000 presidential election debacle. But fears about the security vulnerabilities inherent in DRE machines have caused the state legislature to consider implementing a paper record requirement that may render their four-year old system obsolete. A new law will allow Georgia to launch a pilot program in a few precincts using machines fitted to print a voter verified paper ballot.⁴⁴

Furthermore, Maryland's Governor Robert Ehrlich, a long-time proponent of the state's system of Diebold machines, called for a paper ballot requirement earlier this year. The Maryland House of Representatives unanimously voted to approve Ehrlich's plan to remove the DRE machines for the November elections and replace them with leased optical scan machines.⁴⁵ The proposal fell victim to partisan wrangling and was left unresolved when Maryland's legislative session ended. Maryland is expected to revisit the issue next year.⁴⁶

Citizen and Reform Groups Take Legal Action to Stop States from Buying DRE Systems

Citizens in a number of states have taken legal action to stop election officials from buying DREs. Law suits have been filed in Arizona, California, Colorado, New Jersey, New Mexico, New York and Pennsylvania. For example, Arizona residents filed for an injunction to stop the purchase of two types of touch screens, the Diebold TSx and Sequoia Edge II. The citizens alleged in their complaint that those machines, "are seriously flawed, have a documented history of inaccurately recording and tabulating votes, and are vulnerable to manipulation by hackers."⁴⁷

Citizens in a number

of states have taken legal action to stop election officials from buying DREs. Law suits have been filed in Arizona, California, Colorado, New Jersey, New Mexico, New York and Pennsylvania.



Voter Action, a nonprofit legal organization, is partnering with local law firms throughout the country to provide these efforts with “legal expertise, expert witnesses, legal research and election data analysis.”⁴⁸ They argue that voter verifiable ballots are essential to the integrity of our voting process and suggest that failure to block the purchase and implementation of DREs will impact elections for the entire lifetime of the voting machines.⁴⁹

IV. State DRE Use and the Risk of Compromised Elections

As the November election nears, 37 states will be using DREs either in every precinct, in certain counties, or as an alternative to other voting technologies in various polling places. Because these machines have been known to malfunction and also present significant security concerns, jurisdictions using these machines are at high risk of a compromised election due to DRE failure.

However, this risk is mitigated in some states and counties because the state has either: 1) passed a law requiring that all voting systems produce a paper record that a voter can verify and mandating an audit comparing machine tallies to hand counts of the paper records, or 2) purchased equipment that automatically produces a paper record, although the state has made no formal requirement.

CHART A shows the status of each state regarding the use of DREs and which, if any, security safeguards are in place.

CHART B characterizes states on a risk level from 1 to 3.

A state is considered a low risk state if they do not use DREs but instead use another voting system. A state is also considered low risk if the state uses DREs but the DREs produce a voter verified paper ballot that will be counted in an audit.

A state is considered medium risk if the voting systems produce a paper record but no audit is required. In these states, there will be paper record back ups if machines malfunction, but because there is no audit required, there is no systemic way to detect whether the machines are systematically adding, dropping or switching votes due to programming errors or malicious code.

A state is considered high risk if the DREs are in use but they do not produce a paper record at all. In these states, votes will simply be lost if machines malfunction or votes are compromised due to programming errors or malicious code.

CHART C shows states in which Common Cause recommends that voters choose to vote by absentee ballot if their polling place only uses DREs. These are states with no-fault absentee voting laws in place.

As the November election nears, 37 states will be using DREs either in every precinct, in certain counties, or as an alternative to other voting technologies in various polling places.

CHART A Status of State Voting Systems ¹

State	DRE Voting Systems Used in State ²	Require Voter-Verified Paper Ballot (VVPB)	Bought DRE systems with VVPB (even though no state law)	Require Automatic Audits of Paper Records	Have Not Yet Purchased System with HAVA Funds	Allow No-Fault Absentee Voting
Alaska	YES	YES			YES	YES
Alabama		YES				
Arkansas	YES	Some counties				YES
Arizona ³	YES		YES			YES
California	YES	YES		YES		YES
Colorado	YES	Most counties. All counties by 2010		Most counties. All counties by 2010 ⁴		YES
Connecticut	YES	YES		YES	YES	
Delaware	YES					
District of Columbia	YES					
Florida	YES					YES
Georgia	YES					YES
Hawaii	YES	YES		YES		
Iowa	YES		Some Counties			YES
Idaho		YES				YES
Illinois	YES	YES		YES		
Indiana	YES					
Kansas	YES		Some Counties			YES
Kentucky	YES					
Louisiana	YES					
Massachusetts ⁵					YES	
Maryland	YES					YES
Maine ⁵		YES			YES	YES
Michigan		YES				
Minnesota		YES		YES		
Missouri	YES	YES			YES	
Mississippi	YES		Most counties			
Montana		YES				YES
North Carolina	YES	YES		YES		YES
North Dakota						YES
Nebraska						YES
New Hampshire		YES				
New Jersey	YES	2008				YES
New Mexico		YES		YES		YES
Nevada	YES	YES				YES
New York	YES	YES		YES	YES	
Ohio	YES	YES				YES
Oklahoma						YES
Oregon		YES				YES
Pennsylvania	YES					
Rhode Island						
South Carolina	YES					
South Dakota		YES				YES
Tennessee	YES				YES	
Texas	YES					
Utah	YES	YES				YES
Virginia	YES					
Vermont		YES				YES
Washington	YES	YES		YES		YES
Wisconsin	YES	YES			YES	YES
West Virginia	YES	YES		YES		
Wyoming	YES		YES			YES

Sources: Verified Voting Foundation, Election.org

¹Although we've made every effort to be accurate at the time of publication, there may be subsequent changes not recorded here.

²This means that at least one jurisdiction in the state employs DREs. There may be others that do not use DREs.

³The Arizona legislature recently passed a bill that would require VVPB and mandatory audit for voting machines, but it has not yet been signed into law at the time of publication

⁴All counties are required to perform a post-election audit

⁵These states currently have no DRE systems in place but they have yet to purchase voting machines that will meet the requirements for disabled voters and may choose a DRE system with VVPB. Massachusetts voting systems are not legally required to have a VVPB or a mandatory audit

CHART B State-By-State Voter Risk Assessment

State	Risk Level
Alaska	LOW
Alabama	MID*
Arkansas	HIGH^
Arizona	MID
California	LOW
Colorado	MID#^
Connecticut	LOW
Delaware	HIGH
District of Columbia	HIGH
Florida	HIGH
Georgia	HIGH
Hawaii	LOW
Iowa	HIGH ^
Idaho	MID*
Illinois	LOW
Indiana	HIGH
Kansas	HIGH^
Kentucky	HIGH
Louisiana	HIGH
Massachusetts	MID
Maryland	HIGH
Maine	MID
Michigan	MID*
Minnesota	LOW*
Missouri	MID
Mississippi	MID^
Montana	MID*
Nebraska	MID*
New Hampshire	MID*
New Jersey	HIGH#
New Mexico	LOW*
North Carolina	LOW
North Dakota	MID

State	Risk Level
Nevada	MID
New York	LOW
Ohio	MID
Oklahoma	MID*
Oregon	MID*
Pennsylvania	HIGH
Rhode Island	MID*
South Carolina	HIGH
South Dakota	MID*
Tennessee	HIGH
Texas	HIGH
Utah	MID
Virginia	HIGH
Vermont	MID*
Washington	LOW
Wisconsin	MID
West Virginia	LOW
Wyoming	MID

Chart Key	
Low Risk	Use paper-based system with mandatory audit of machines or DRE System with VVPB and mandatory audit.
Mid Risk	Use paper-based voting systems or DRE voting systems that have VVPB but no audit requirement.
High Risk	DRE systems used without VVPB
*	No DRE systems used
#	DRE systems will have VVPB and will require audits in future
^	Some but not all counties will be using DRE systems with VVPB

PLEASE NOTE: Risk is assessed according to availability of VVPB and mandatory random audits.

DRE - Direct Record Electronic
VVPB – Voter Verified Paper Ballot

CHART C Mid-and High-Risk States That Allow No-Fault Absentee Voting

<u>State</u>	<u>Allow No-Excuse Absentee Voting</u>	<u>Risk Level</u>
Arkansas	Yes	HIGH
Delaware		HIGH
District of Columbia		HIGH
Florida	Yes	HIGH
Georgia	Yes	HIGH
Iowa	Yes	HIGH
Indiana		HIGH
Kansas	Yes	HIGH
Kentucky		HIGH
Louisiana		HIGH
Maryland	Yes	HIGH
New Jersey	Yes	HIGH
Pennsylvania		HIGH
South Carolina		HIGH
Tennessee		HIGH
Texas		HIGH
Virginia		HIGH

In those states marked “yes” in the chart above, Common Cause recommends voting by absentee ballot if voters’ only other option in their precinct is a paperless DRE.



Recommendations

Congress passed the Help America Vote Act (HAVA) in 2002 to rectify problems in our election system exposed during the 2000 presidential election. Plagued by the memory of election officials haggling over hanging chads, Congress included requirements calling for technological advances in election system machinery.

Many election officials perceived DREs as the best answer to some HAVA requirements. As a result, DRE use exploded. The number of counties nationwide using DREs more than tripled in the last six years, jumping from 320 counties in November 2000 to an expected 1,050 counties in November's mid-term elections. About 39 percent of registered voters are expected to use DRE voting machines on Election Day 2006.

However, because these machines are proven to be prone to malfunction and failure and vulnerable to computer hacking, it is clear that we must take bold action to safeguard our elections, or it is likely that they will be compromised. Transparent methods for proving the accuracy of election tallies will help reassure voters that the election results are correct.

Common Cause recommends the following steps to mitigate the risks caused by DRE machines and to create long-term solutions to protect election integrity:

Congress must immediately pass HR 550, "The Voter Confidence and Increased Accessibility Act of 2005." Representative Rush Holt (D-NJ) last year re-introduced his "Voter Confidence and Increased Accessibility Act of 2005," a bill that would require all voting machines to produce a voter-verified paper record and to be subject to routine unannounced audits by hand-count. Common Cause fully supports HR 550 and encourages citizens to contact their members of Congress to co-sponsor the bill. Currently, there are 191 co-sponsors of this bill from both parties.

States should pass laws or adopt regulations requiring all voting systems to produce a voter verified paper ballot and mandate that at least two percent of voting jurisdictions, randomly selected, conduct public audits of their voting systems. In the past few years, 27 states have enacted laws or adopted administrative rules requiring voting systems to produce voter-verifiable paper records. However, only 15 of those states also require an audit of the voting system to ensure accuracy. Without an audit to compare computer tallies to manual tallies of voter verified paper records, there is no way to know if the voting machine is malfunctioning [note: malfunctions may show up but they can't be resolved and, in some cases, they may not show up at all], whether due to programming errors or malicious code. Unless and until a federal law such as HR 550 is passed, states must individually safeguard their voting systems.

Many election officials perceived DREs as the best answer to some HAVA requirements. As a result, DRE use exploded. The number of counties nationwide using DREs more than tripled in the last six years, jumping from 320 counties in November 2000 to an expected 1,050 counties in November's mid-term elections.

States and localities must take necessary steps to safeguard machines prior to use. Jurisdictions must implement security plans to ensure the machines are guarded and only authorized persons are able to program and retrieve information from the machines. Poll workers need proper training on the use of new equipment. Pre- and post-election tests must be performed to ensure the voting systems are working accurately. Local election officials should make emergency paper ballots available to voters in case of machine malfunction.

State election officials should, where possible, retrofit DREs with printing systems to produce a voter verifiable paper ballot, and use those ballots in audits. Common Cause realizes that certification rules may stand in the way of this change. However, we offer this advice: “Where there’s a will, there’s a way.” The certification process can be expedited.

When DREs cannot be retrofitted, Common Cause recommends that state election officials decertify those DREs that cannot provide a paper record and turn to other election systems such as optical scan machines for use in the November elections. Paperless DREs are unacceptable for use in a system that relies on the confidence of voters for its legitimacy.

Common Cause recommends that emergency funds be made available to states for the purchase or lease of more secure, auditable machines.

Because they lack the funding to acquire new machines, many election officials may assume that it’s impossible to retrofit or discard their DREs and switch to better technology. Secure, verifiable elections are worth the investment.

Common Cause recommends that citizens be aware of the voting systems in use in their locality. If a polling place is equipped with a paperless DRE, voters may seek to vote on a paper ballot. Given that paperless DREs present the highest security risk, Common Cause urges voters to identify what kind of voting equipment is used at their polling place. Voters can their secretary of state’s office, county clerk, registrar, or local board of elections. Voters who discover that their polling place will use voting machines with no voter-verifiable paper record should vote by absentee ballot, if their state allows no-excuse absentee voting [see chart C on page 21]. Voters who will vote by absentee ballot should check with their Secretary of State’s office to make sure they are aware of the rules around absentee voting. For example, there may be deadlines and requirements for witnesses and other criteria.

If voters find themselves in a precinct using DREs in a state that doesn’t allow no-excuse absentee voting, Common Cause urges those citizens to first work with advocacy groups to demand—well before the election—that local election officials make emergency paper ballots available on Election Day in case of machine malfunction. Citizens can also request that paper ballots be made available for any voter who doesn’t wish to vote on a DRE. However, citizens should not accept the option of voting on a “provisional ballot,” which is not accorded the same status as the ballot of a voter who is properly registered and whose name appears on the voter rolls

Common Cause

recommends that emergency funds be made available to states for the purchase or lease of more secure, auditable machines.

-
- ¹ Public Law No. 107-252, The Help America Vote Act of 2002
- ² Press Release. "First in Bay Area: Alameda County to Introduce Touch-Screen Voting from Diebold Nov. 5," Diebold via *Business Wire*, Sept. 18, 2002
- ³ Press Release. "69 Million Voters Will Use Optical Scan Ballots in 2006: 66 Million Voters Will Use Electronic Equipment," Election Data Services, Feb. 6, 2006
- ⁴ Thompson, Clive. "A Really Open Election," *The New York Times*, May 30, 2004
- ⁵ Rubin, Avi. Testimony before the U.S. Election Assistance Commission, May 5, 2004 (see <http://www.eac.gov/docs/Testimony%20-%20Avi%20Rubin.pdf>)
- ⁶ Trusted Agent Report. Diebold AccuVote-TS System, by RABA Innovative Solution Cell (RiSC), January 2004
- ⁷ Risk Assessment Report. Diebold AccuVote-TS Voting System and Processes, by Science Applications International Corporation, Sept. 2, 2003
- ⁸ Government Accounting Office. "Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Underway, but Key Activities Need to Be Completed" (GAO-05-956), September 2005, p. 2
- ⁹ *Ibid*, p.53
- ¹⁰ Commission on Federal Election Reform. "Building Confidence in U.S Elections," September 2005
- ¹¹ Hursti, Harri. "Critical Security Issues with Diebold TSx, A Black Box Voting Project," May 11, 2006
- ¹² Rubin, Avi. "Security Risk Seen in Diebold Voting Machine," Weekend Edition, National Public Radio, May 20, 2006
- ¹³ Davey, Monica. "New Fears of Security Risks in Electronic Voting Systems," *The New York Times*, May 12, 2006
- ¹⁴ Desmon, Stephanie. "Experts See New Diebold Flaw," *The Baltimore Sun*, May 12, 2006, <http://www.securityfocus.com/news/11391>
- ¹⁵ Lemos, Robert. "Diebold Voting Systems Critically Flawed," Security Focus, May 12 2005. <http://www.securityfocus.com/news/11391>
- ¹⁶ Tinsley, Anna and Spangler, A. "Vote Spike Blamed on Program Snafu" *Fort Worth Star-Telegram*, March 9, 2006
- ¹⁷ Tinsley, Anna. "Judicial Candidate Files Challenge" *Fort Worth Star-Telegram*, April 6, 2006
- ¹⁸ Robertson, Gary. "Troxler to Take Commissioner's Post After Cobb Concedes," *Associated Press*, Feb. 4, 2005
- ¹⁹ Bonner, Lynn. "Cartaret Elects to Ditch Voting Machines," *The News & Observer*, July 15, 2005
- ²⁰ Press Release. "Secretary of the Commonwealth Decertifies Unilect Patriot Voting System in Pennsylvania," Pennsylvania Department of State, April 7, 2005
- ²¹ Walter, Kori. "Vote Machines Will Work Well, Supplier Says," *Reading Eagle*, Nov. 3, 2005
- ²² Editorial. "Board Should Hold a Revote for the City," *Reading Eagle*, July 20, 2005
- ²³ Schwartz, Noaki and Negrete, Tere. "Voting Glitches Found in 6 Recent Elections," *Miami Herald*, March 31, 2005
- ²⁴ Schwartz, Noaki and Negrete, Tere. "Dade Election Chief Kaplan Resigns," *Miami Herald*. April 1, 2005
- ²⁵ Kidwell, David. "Dade Could Resume Low-Tech Voting," *Miami Herald*, May 29, 2005
- ²⁶ Cho, David. "Fairfax Judge Orders Logs of Voting Machines Inspected," *The Washington Post*, Nov. 6, 2003
- ²⁷ *Ibid*.
- ²⁸ VotersUnite.org: (see <http://www.votersunite.org/article.asp?id=3421>)
- ²⁹ Zoretich, Frank. "Election Results Certified After Software Blamed," *Albuquerque Tribune*, Nov. 19, 2002
- ³⁰ "12,000 Early Votes Skipped in Count," *Albuquerque Tribune*, Nov. 16, 2002.
- ³¹ Cohen, Robert. "Key Reforms Won't Be in Place for 2004 Elections," *Newhouse News Service*, May 28, 2003
- ³² Keller, Amy. "Questions Swirl On Voting Reform," *Roll Call*, March 25, 2004
- ³³ <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00550>:
- ³⁴ Yachnin, Jennifer. "Ehlers Named 'Mayor'; New Chair for House Administration," *Roll Call*, January 18, 2006
- ³⁵ Anselmo, Joseph. "Physicist Ehlers Is the Go-To Guy on Science Matters," *Congressional Quarterly Daily Monitor*, June 24, 2003
- ³⁶ Rep. Ehlers. Statement during a town hall meeting at the Gerald R. Ford Museum in Grand Rapids, MI. May 6, 2006
- ³⁷ Riley, Brandon. "Nevada Decides on New Voting Machines" *Associated Press*, Dec. 10, 2003
- ³⁸ News Release. "Secretary of State Heller Announces Direct Recording Electronic Voting Machine Choice," Nevada Office of the Secretary of State, Dec. 10, 2003
- ³⁹ News Release. "Secretary of State Kevin Shelley Bans Diebold TSx for Use in November 2004 General Election," Office of the California Secretary of State, April 30, 2004
- ⁴⁰ Vogel, Nancy and Rau, Jordan. "Governor Returns Primary to June; Signature on Bill Ends a Futile Effort to Increase the State's Clout in Presidential Elections" *Los Angeles Times*, Sept. 28, 2004
- ⁴¹ Kravets, David. "Voters Sue to Keep Diebold From Elections," *Associated Press*, March 22, 2006
- ⁴² Massey, Barry. "Governor Proposes Standardized Paper Ballot System Statewide," *Associated Press*. Jan. 12, 2006
- ⁴³ Baker, Deborah. "Governor Signs Paper Ballot Bill Into Law," *Associated Press*, March 3, 2006
- ⁴⁴ Campos, Carlos. "Georgia's 4-Year Old Voting Devices Looking Old. They're Paperless, and That's the Problem," *Atlanta Journal Constitution*, April 30, 2006
- ⁴⁵ Marimow, Ann. "Maryland House Approves Paper Ballots," *The Washington Post*, March 10, 2006
- ⁴⁶ Brewington, Kelly. "Paper Ballot Crumbling: Electronic Voting Machines Seem Likely to be Retained," *The Baltimore Sun*, April 7, 2006
- ⁴⁷ Chavez v. Brewer (Arizona Superior Court Maricopa County, May 9, 2006) (see <http://www.voteraction.org/States/Arizona/Documents/Legal/MtnPrelim%20Injtcn.pdf>)
- ⁴⁸ Voter Action: <http://www.voteraction.org/about.html>
- ⁴⁹ Voter Action: <http://www.voteraction.org/States/California/CA.html>
-