To: Nathaniel Persily
From: Kyle Rifkind and Samuel Eisenberg
Re: Voting Machine Capacity and Technology
Date: May 23, 2013

INTRODUCTION

This memo summarizes the current literature on issues regarding voting system technology. The majority of jurisdictions in the United States use either optical scan or digital recording equipment (DRE) voting systems. Each type and model voting machine represents a trade-off between cost, usability, reliability, and security. This memo begins with an overview of the recent history of voting machines and the types used in the United States, then discusses reported issues of malfunctioning voting machines and security risks to electronic voting systems and the vote counting process. The memo concludes with proposed solutions, recommendations, and best practices. An annotated bibliography follows.

Federal statutory background

In the wake of the 2000 election, Congress passed the Help America Vote Act (HAVA), which established standards for voting equipment (42 U.S.C. § 15481):

- Voting systems must notify the voter when he selected more than one candidate for a single office on the ballot;
- Voting system must notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office;
- Voting system must provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.

HAVA also provided significant funding for states and counties to purchase new voting machines (Lawyer's Committee for Civil Rights Under the Law, 2013; Charles Stewart III, 2013):

- Most jurisdictions at the time of HAVA did not have electronic voting systems, relying instead on punch cards, lever machines, and hand counted paper ballots. But with the new HAVA standards and HAVA money, jurisdictions purchased more technologically advanced voting systems—direct recording equipment (DRE) machines and optically scanning paper ballot systems.
- HAVA funding was not continuously provided but rather was a lump sum disbursement; jurisdictions that initially purchased the expensive new voting systems did not have money to repair them as they inevitably broke or wore down, to purchase new machines when the initial ones became obsolete, or to add new machines as their population grew.
- After HAVA, jurisdictions mostly purchased DRE machines but after a few years of explosive growth most local election officials stopped adopting more DRE machines because of security concerns and the expense of maintaining DRE machines.
- In place of DRE machines, election officials have purchased optical scanners and nearly abandoned punch cards, lever machines, and hand counted paper ballots completely, so

that by the 2008 election 58% of voters were using optical scanners and 30% were using DRE machines.

- The differences in technology adoption are driven by when the locality purchased the machines (purchases in the early 2000s more likely to be DREs, those in the mid to late 2000s more likely to be optical scanners), state laws that mandate a certain kind of technology, and county size (larger counties more likely to use optical scanners), but not racial composition or median income.

Significantly, HAVA also created the United States Election Assistance Commission (EAC):

- The EAC collects nationwide election data and promulgates guidance for HAVA compliance.
- The EAC also certifies voting systems and accredits labs that test voting systems.
- HAVA's Technical Guidelines Development Committee published Voluntary Voting System Guidelines in 2005, although these were not approved by the EAC. Those guidelines build on voluntary standards from the Federal Election Commission, published in 1990 and updated in 2001.

Voting systems

U.S. jurisdictions currently use four types of voting systems (Verified Voting Foundation):

- Optical Scan Paper Ballot Systems
    - Voters mark paper ballots by filling in bubbles or connecting ends of an arrow. The ballots are counted by optical scanning machines, either at each precinct or at a central location.
- Direct Recording Equipment (DRE) Systems
    - The voter uses buttons or a touchscreen to make selections. Votes are recorded into computer memory on a cartridge, diskette, or smart card.
    - Some DRE machines have Voter Verified Paper Audit Trail systems, which print a record of the voter's selections in real time, allowing the voter to confirm their choices before they are stored in memory. The paper record is stored by election officials, and can be used for recounts or audits. (See, e.g., Verified Voting Foundation, "Hart Intercivic eSlate" or "ES&S iVotronic" for explanations and video examples).
- Ballot Marking Devices
    - To assist voters with disabilities, these systems translate inputs on a touchscreen or buttons into marks on a paper ballot, which can then be scanned or hand counted. Ballot marking systems have audio interfaces and other accessibility features.
- Hand Counted Paper Ballots
    - Ballots marked by voters are counted by hand. Manual counts are still used in some jurisdictions as a primary method or for counting absentee ballots; paper ballots may also be hand counted in a recount.

Two additional types of systems have largely been phased out after HAVA:

- Punch Card Voting Systems
    - Voters punch holes in a card that is aligned in the machine with a list of candidates. The cards are then counted by computer. As of 2012, punch card systems were used by only four counties in Idaho.
- Mechanical Lever Voting Machines
    - Voters make selections using a series of switches, and then throw a master lever to cast their votes, which are recorded by incrementing mechanical rotors. Lever machines are no longer used in the United States.

Research in California, Maryland, North Carolina, Miami Dade County, FL, and Butler County, OH found that the cost of implementing optical scan systems was less than for DRE systems. (Pew 2012).

- For example, Miami-Dade County estimated it could save $13 million over five years by switching from DRE to optical scan systems.

Residual vote rate

The residual vote rate is a metric, based on the number of ballots that fail to contain a legitimate vote, that can be used to evaluate the comparative performance of election systems (Charles Stewart III, March 2013)

- The number of residual votes for a given race is calculated by adding the number of overvotes, where the voter selects too many candidates for a given race, to the number of undervotes, where the voter selects too few candidates for a given race. The residual vote rate is the number of residual votes divided by total turnout for the given race.
- While the residual vote rate is an effective metric at comparing the performance of particular voting machine technologies it is not able to disaggregate the source of a problem among user error, machine malfunction, or precinct mistake.
- In a study of the 2008 presidential election, it was found that DRE machines and optical scanners had similar levels of low residual votes. While precincts with DRE machines had longer lines than those with optical scanners, the difference had little to do with the DRE machines themselves, and rather to do with the types of communities that are most likely to have DRE machines. Also, voters had lower confidence in DRE machines than optical scanners, with the confidence difference more pronounced among liberals than conservatives.
- The national residual vote rate has dropped over time, from 1988 to 2008, in part because punch card machines have been replaced with DRE machines and optical scanners which prompt voters when they make errors.

SCOPE OF THE PROBLEM

Malfunctions

Existing state laws can make it difficult to purchase new or additional voting equipment or to deal with election day problems:

- Some current state laws prohibit jurisdictions from replacing DRE machines as they break down or as additional machines are needed to keep pace with growing voter population. And some state laws also prohibit local election officials from distributing emergency paper ballots if there are any functioning DRE machines in a precinct. That means that if some machines break down, creating long lines and voter frustration, local election officials cannot use emergency paper ballots unless all of the machines in the precinct malfunction. (Lawyers' Committee for Civil Rights Under the Law, 2013).

The wait time for optical scanning equipment in the 2008 presidential election was about 11 minutes, DRE machines was about 17 minutes, lever machines was about 8 minutes, and hand counted paper was about 2 minutes.

Sources of delay or malfunctions for DRE machines (ABA Standing Committee on Election Law, May 2013):

- Too few machines in a precinct both at the beginning of election day and as machines inevitably break; lack of replacements or fixes available.
- Machines breaking because the screen freezes, unexpectedly shuts down, or flips a voter's choice so that the machine registers a different choice than the one the voter intended.
- Machines are expensive so they are more difficult to add when turnout is high or population grows.
- Poorly training poll workers who provide inaccurate advice, do not know how to fix machines that malfunction, or who do not know how to audit the paper trail properly.
- Voters not having confidence in a particular type of technology because of previous poor experiences with that type of machine, second hand accounts of malfunctions with that type of machine, or distrust of technology generally especially touchscreen machines. This leads to long lines as voters wait for their preferred machines, often paper ballots or optical scanners.

Sources of delay or malfunctions for optical scanners (ABA Standing Committee on Election Law, May 2013):

- Too few machines in a precinct both at the beginning of election day and as machines inevitably break; lack of replacements or fixes available.
- Too few paper ballots so that if turnout at a precinct is higher than expected it can run out of physical ballots.
- Machines breaking because they jam while scanning the paper ballot.
- Poorly training poll workers who provide inaccurate advice, do not know how to fix machines that malfunction, or who do not know how to audit the paper trail properly.

- Long ballots means it takes local election officials more time to scan, which can cause delays.

Lack of information sharing (Brennan Center, 2010):

- Repeatedly the same problems afflict the same systems but in different jurisdictions in different elections, yet local election officials have no central location where they can find comprehensive information about problems discovered with their system before each election.
- The EAC reporting regime requires voting system vendors to report "malfunctions" of EAC certified systems. Malfunction is defined as "a failure of a voting system, not caused solely by operator or administrative error, which causes the system to cease operation during a Federal election or otherwise results in data loss." Malfunction reports are posted on EAC's website.
- Notification of malfunctions to EAC are only required for federal elections, and only for specific types of malfunction. For example, malfunctions that occur in testing prior to an election may not be reported.
- Currently election officials rely nearly exclusively on vendors to disclose malfunctions, vulnerabilities, and problems that the vendors have discovered themselves or have had reported to them by other election officials.
- Usually vendors have no legal obligation to notify election officials, a federal agency, or the public about problems with their systems, and in fact, they usually have strong economic incentives to hide evidence of their systems malfunctioning.
- Had election officials known about the vulnerabilities their machines face and the common problems with their machines along with proven solutions, they would be able to prevent issues from arising and resolve them more quickly.

Security Concerns

Each type of voting system technology introduces security risks into the system, as do procedures for maintaining chain of custody over the systems, oversight and training of election officials, and other human factors. While the media has focused on the real risks of "hacking" of computerized systems and the lack of auditable paper trails for certain DRE systems, there are security risks to every voting system, including those that use paper ballots. There are risks and trade-offs between security, auditability, usability, and cost across different systems and procedures.

Security Vulnerabilities

Possible security risk pathways include:

- Physical access, especially vulnerable components such as memory cards and computer ports;
- Computer system access, via either physical or cyber attack;
- Vulnerability to computer viruses;

- Hardware errors;
- Software errors;
- Cryptography;
- Human error;
- Chain of custody;
- Manipulation by poll workers.

A malicious attack could exploit a vulnerability to produce a variety of different types of fraudulent actions or errors, such as:

- Miscounting of votes;
- Manipulation of vote totals during or after voting;
- Violations of voter privacy;
- Causing systems to crash or become unusable;
- Premature voting or ability to vote abandoned ballots.

In recent years, multiple groups have documented successful hacking attacks against electronic voting systems (Caltech/MIT 2012):

- A U.C. Berkeley team found, as part of California's "top-to-bottom" review of its voting systems, that Sequoia AVC Edge DRE machines lacked data integrity safeguards, used flawed or imperfectly implemented cryptography, had ineffective computer access control mechanisms, and contained "numerous" programming errors that created or expanded vulnerabilities. (Blaze et al. 2007).
- An expert-witness report by Princeton researchers for litigation in New Jersey found Sequoia AVC Advantage DRE systems could hacked to steal votes by replacing a machine's firmware. The hack could be accomplished by an attacker with only "ordinary training" in computer science, took seven minutes to execute, could spread virally through machines in a precinct, could be used to manipulate vote tallies or divulge voters' choices, and was practically undetectable. (Appel et al. 2008).
- In 2011, researchers at Argonne National Laboratory demonstrated three types of attacks on Diebold touchscreen DRE machines. These hacks required less than $30 in parts and were untraceable. The researchers noted the need to focus on physical security of electronic voting machines as well as "cyber" threats. (Vulnerability Assessment Team website; Friedman 2011).
- Wagner et al. (2006) found serious but fixable security vulnerabilities in the AccuBasic language interpreter for two types of Diebold optical scan and touchscreen systems. An attacker could insert code allowing him to control the system or modify results by accessing the machines' memory cards. These attacks would not be discoverable without examination of the paper ballots.
- Feldman et al. (2007) also found Diebold machines "vulnerable to extremely serious attacks," including the ability of a hacker to insert malicious code that could spread to other machines in the course of normal operation. The study concluded that changes were needed to the hardware and software of the machines, as well as to the procedures

for using the machines, to fix the vulnerabilities.

- However, vulnerabilities to electronic voting machines may also apply to the electronics used to count paper ballots in optical scan systems. (Alvarez and Hall 2010).

As with the reporting of system malfunctions, the current reporting regime fails to protect and inform voters and election officials about security threats.

- There is no central clearinghouse where jurisdictions can obtain information about security risks to the systems they use, and vendors are not required to disseminate information about discovered threats to all jurisdictions using a particular system. (Brennan Center 2010).

The current federal certification regime is also inadequate.

- The EAC notification regime only applies to EAC certified systems. The EAC did not start certifying voting systems until 2009, only around 1% of U.S. jurisdictions use EAC certified systems as of 2010. Most states do not have funding available for the purchase of new system, since most systems were purchased earlier in the decade through HAVA.
- Further, most states do not require than new equipment be EAC certified. (Brennan Center 2010). Certification alone, of course, does not provide any safeguard against misuse of or tampering with machines, human error such as incorrect programming, or undetected exploits. (Caltech/MIT 2012).

Auditing

Post-election audits are methods to test the integrity of vote counting systems. Auditing methods include verification of reported precinct vote counts, inspection of voting machines, and comparing results from electronic voting systems to paper audit trails or ballots. A full manual recount of paper ballots would constitute the most thorough audit, but is also the most costly. For a given margin of victory, random testing of a smaller sample of ballots or machines can audit an election to a specified level of statistical confidence at reduced cost. (Aslam et al. 2008).

- Currently at least half of the states conduct some type of post-election audit. Post-election auditing may be less costly than pre-election certification of voting systems. (Caltech/MIT 2012).
- For example, California law requires that 1% of all precincts are audited. A random process for choosing which precincts to audit adds security. However, large jurisdictions are sometimes notified of their selection before they have finished initial tallies of, for example, absentee ballots. (Hall 2008).
- For jurisdictions with DRE systems, the only possible post-election audits are verifying that the totals in memory were reported correctly and inspecting voting machines for evidence of tampering. As of 2008, twelve states allow voting systems that do not produce any paper record. (Hall 2008).
- Statistical auditing methods can reduce costs. For example, the sample size for an audit can be varied by the size of the precinct being audited. (Aslam et al. 2008) Statistical methods can ensure at a given confidence level that errors will be found if they exist. If

errors are found, the size and scope of the audit can be increased until the auditor is able to confirm or reject the reliability of the outcome. (Stark 2008).

- Requiring paper audit trails may frustrate the development of other solutions; technological and cryptographic solutions may prove better than paper audits for auditability and verifiability. (Alvarez and Hall 2010).

The Caltech/MIT Voting Technology (2012) report notes several trends in voting system security over the past decade:

- "A strong movement away from all-electronic voting systems, toward voting systems based on paper ballots: Increased interest in post-election auditing; Strong interest from computer security experts and cryptographers in the problems of voting system security; Some jurisdictions (such as Travis County, Texas) taking the design of voting systems into their own hands, in consultation with expert advisory boards."
- However, the report also notes several trends it finds worrying, including increased interest in voting by mail and over the internet; auditing challenges posed by ranked-choice and instant-runoff voting systems; problems with the federal certification; and problems with centralization, transparency, and research and development among voting system vendors.
- Overall, the Caltech/MIT authors find it difficult to conclude whether election security has improved since 2000, due to a lack of systematic data. While the incidence of federal prosecutions suggests low incidence of fraud (bolstered by statistical studies such as Mebane 2008), the problem has not been sufficiently studied. (Caltech/MIT 2012)

POTENTIAL SOLUTIONS

Malfunctions

Number of voting machines (ABA Standing Committee on Election Law, May 2013):

- Relax state laws that prohibit jurisdictions from purchasing new machines or new kinds of machines.
- Spend money to purchase more machines to have backups in the case of election day failures that cannot be fixed and to ease long lines that inevitably build up on election day.
- Shift resources to purchasing more optical scan paper ballot systems and away from DRE machines because the former are less expensive, more reliable, and more auditable.

Emergency paper ballots (ABA Standing Committee on Election Law, May 2013):

- Relax state laws that prohibit jurisdictions from distributing emergency paper ballots when some, rather than all, DRE machines in a precinct malfunction.
- Ensure that the paper ballots are labeled as emergency ones that are not confused with provisional or absentee ballots.

More effective voting machine messages (Brennan Center, 2012):

- When voters undervote or overvote the voting machine should prompt the voter with a clear message written in plain English that the voter has selected too many (overvote) or too few (undervote) choices for a particular race and the consequences of their action (vote will not be counted).
- Ideally the voting machine system will not permit the voter to proceed to the next race or submit their ballot without correcting the overvoting error (this should not be extended to undervoting errors because voters may have legitimate reasons for abstaining from a particular race).
- The key to an effective message is immediate feedback that is easily comprehensible based on design and language.

Creation of a national database (Brennan Center, 2010):

- A new federal regulatory system centered on a national clearinghouse for voting system problems that is publicly available, searchable, and comprises election official, vendor, and voter reported problems.
- Vendors must be legally required to report to the database and appropriate agency known or suspected failures and vulnerabilities, customer complaints, warranty claims, and remedial actions taken.
- Empower a federal agency such as the EAC to investigate voting system malfunctions and vulnerabilities, give the agency subpoena power, allow it to require that vendors keep records of known or suspected problems, and allow the agency to assess penalties for noncompliance.

Interim national database (Brennan Center, 2010):

- Should the mandatory national database not be feasible or take a long time to implement, election officials in the meantime can negotiate better contracts with vendors that requires them to disclose problems that other election officials report to them.
- Election officials can agitate for states or vendors to create their own databases or the federal government can create a voluntary one.

Security Concerns

Use of Comprehensive Risk Assessments:

- Election risk assessments should cover all aspects of the election process, including both voting machines and human processes (for example, the Sandia National Laboratories Vulnerability Assessment Model). (Alvarez and Hall 2010).
- Hold all voting systems to the same level of threat-risk scrutiny. (Alvarez and Hall 2010).
- Keep in mind that applying technological solutions to one problem may introduce other problems. (Bishop and Wagner 2007).
- "De-emphasize standards for security, aside from requirements for voter privacy and for auditability of election outcomes." Beyond minimal security standards, substitute post-election auditing for more thorough equipment certification. (Caltech/MIT 2012).

Software Independence

- A "software independent" system is defined as one where a software error cannot cause an undetectable error in an election outcome.
- "This notion was proposed for adoption as part of the federal voting system certification standards (2005 Voluntary Voting System Guidelines). The notion does not exclude the use of software, but recognizes the extraordinary difficulty of producing correct software, by requiring that election outcomes produced by software-based voting systems be checkable by other means; the simplest software- independent approach is to complement such systems with voter-verifiable paper ballots." (Caltech/MIT 2012).

End-to-End Voting Systems

- End-to-end voting systems allow the voter to verify that his vote was cast as intended, allow the voter to verify that the vote was recorded as cast, and allow anyone (for example, election officials, candidates, or courts) to verify that a vote was tallied as recorded. These systems typically use encryption to allow voters to check that their votes were correctly tallied. Such methods are beyond current system capabilities. (Caltech/ MIT 2012).

Auditing

- Use mandatory compliance and risk-limiting audits, with a focus on regulation of the election evidence trail. (Stark and Wagner 2012).
- Holistic auditing of the entire election process, including both vote counting systems and the procedures used by election officials.
- For post-election audits, use statistical methods to ensure both the detection of errors in vote counting and the reliability of election outcomes. (e.g., Stark 2008).

Improved Federal Standards (Caltech/MIT 2012):

- Harmonize voting system requirements across states, to reduce costs and create a less fragmented market.
- Standardized, public formats for data generated by voting systems.
- A central clearinghouse for best practices and reporting of security threats and fixes.
- Ownership of data by jurisdiction and election officials, rather than vendors.
- An emphasis on ensuring auditable and verifiable elections, and the creation of uniform standards for audits.
- Standardize best practices for chain of custody and election day operating procedures. (Alvarez and Hall 2008).

Funding and R&D:

- Increased funding for research into election systems and election forensics.
- Research should attempt to address three essential questions: "To what extent has fraud occurred in previous elections?; Are voting systems returning the correct election outcome?; Are voting systems providing good evidence for the correctness of the election outcomes they are reporting? Is the outcome verifiable?" (Caltech/MIT 2012).

- Tapping the knowledge and resources of America's computing and information technology industries, which have so far stayed out of the voting systems business.

BIBLIOGRAPHY

Verified Voting Foundation, "Verified Voting," https://www.verifiedvoting.org/. Provides an overview of voting systems and election audits. Lists and provides a map of voting technologies by state and county (https://www.verifiedvoting.org/verifier/). Discusses individual voting machines, including setup, usage, security risks, and known attacks. Includes videos from manufacturers and/or jurisdictions demonstrating voting on various types and models of electronic voting systems.

Voting: What Has Changed, What Hasn't, and What Needs Improvement, Caltech/MIT Voting Technology Project (2012, updated Jan. 14, 2013) ("Caltech/MIT 2012), http://www.vote.caltech.edu/sites/default/files/Voting%20Technology%20Report_1_14_2013.pdf
This source provides an overview of security issues with voting systems, including trends since the previous Caltech/MIT report in 2000. It discusses the evolution of federal standards and state practices, and offers regulatory, business, and technical recommendations for improving election security.

Lawyers' Committee for Civil Rights Under Law, The 2012 Election Protection Report: Our Broken Voting System and How to Repair It (2013). http://www.866ourvote.org/newsroom/publications/document/EP-2012-Full-Report.pdf
This source describes HAVA and details the onerous restrictions that Virginia law places on the use of emergency paper ballots when only some DRE machines break on election day, on replacing broken DRE machine with new ones, and purchasing more machines as population grows.

ABA Standing Committee on Election Law, Election Delays in 2012 Report (May 2013). http://www.americanbar.org/content/dam/aba/administrative/election_law/2012_election_delays_report.authcheckdam.pdf
This source describes HAVA and summarizes the most common sources of DRE machine and optical scanner malfunctions and delays during the 2012 election. The source then goes on to propose numerous solutions to the problems associated with DRE machines and optical scanners.

Brennan Center for Justice, Better Design, Better Elections (2012). http://www.brennancenter.org/sites/default/files/legacy/Democracy/VRE/Better_Design_Better_Elections.pdf
This source focuses on how ineffective voting machine messages can result in significant, avoidable overvotes and undervotes despite the HAVA standards.

Brennan Center for Justice, Is America Ready to Vote? State Preparations for Voting Machine Problems in 2008 (2008). http://www.brennancenter.org/sites/default/files/legacy/publications/is.america.ready.to.vote.pdf
This source describes the best practices of states regarding polling place contingency plans, ballot accounting and reconciliation, voter verifiable paper records, and post-election audits.

The Pew Center on the States, The Help America Vote Act at 5 (2007). http://www.pewstates.org/uploadedFiles/PCS_Assets/2007/HAVA.At.5.pdf
This source describes the evolution of voting machine technology and the problems associated with them in light of HAVA.

Lawrence Norden, Brennan Center for Justice, Voting System Failures: A Database Solution (2010) ("Brennan Center 2010"). http://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf
This source focuses on the fact that the same problems regularly afflict the same machines but in different jurisdictions in different elections yet there is no way for local election officials to learn from their peers. To remedy this problem it proposes the creation of a national clearinghouse database and accompanying federal regulatory agency to enforce it so that election officials, vendors, and voters can submit potential problems and workable solutions. The source also explains why the EAC and its Voting System Testing and Certification Program is inadequate in terms of funding and regulatory authority. Includes fourteen case studies of voting machine failures between 2002 and 2010.

Brennan Center for Justice, Design Deficiencies and Lost Votes (2011). http://www.brennancenter.org/sites/default/files/legacy/Democracy/Design_Deficiencies_Lost_Votes.pdf
This source provides a case study of how ineffective ballot design and electronic voting machine messaging can lead to a substantial number of entirely preventable overvotes while still meeting HAVA requirements.

Charles Stewart III, Election Technology and the Voting Experience in 2008 (March 2009). http://web.mit.edu/cstewart/www/papers/stewart_midwest2009.pdf
This source compares the effectiveness of DRE machines and optical scanners based on residual votes and wait times and probes the underlying causes of the observed differences.

Charles Stewart III, The Performance of Election Machines and the Decline of Residual Votes in the US, in The Measure of American Elections (Barry C. Burden and Charles Stewart III, eds.) (forthcoming 2013). This source gives a comprehensive overview of the residual vote rate, the comparative performance of DRE machines and optical scanners on the basis of residual votes and wait times over time, and the changes in voting machines since HAVA.

Paul Gronke et al., Residual Voting in Florida (October 2010). This source describes the residual vote rate metric and provides a case study of the 2008 election in Florida to measure the effectiveness of DRE machines and optical scanners.

Thad E. Hall, and R. Michael Alvarez. 2008. "Building Secure and Transparent Elections Through Standard Operating Procedures." Caltech/MIT Voting Technology Project, Working Paper 65, https://www.vote.caltech.edu/content/building-secure-and-transparent-elections-through- standard-operating-procedures-0. Discusses standard operating procedures and chain of custody issues in elections from legal and administrative perspectives; focuses on security, fraud prevention, and transparency. Includes case studies.

Joseph Lorenzo Hall, "Improving the Security, Transparency and Efficiency of California's 1% Manual Tally Procedures" (2008), http://static.usenix.org/event/evt08/tech/full_papers/hall/hall_html/. Discusses lessons learned from California's post-election audit process.

David Wagner et al., Security Analysis of the Diebold AccuBasic Interpreter (2006), http://nob.cs.ucdavis.edu/bishop/notes/2006-inter/2006-inter.pdf

Matt Bishop and David Wagner, Risks of E-voting, Inside Risks 209, CACM 50, 11 (2007) http://www.csl.sri.com/users/neumann/insiderisks07.html#209. Discusses lessons learned from California's top-to-bottom review of its voting systems, including system vulnerabilities and the interplay with current federal regulations.

Peter G. Neumann, U.S. Election After-Math, Inside Risks 217, CACM 52, 2, February 2009, http://www.csl.sri.com/users/neumann/insiderisks08.html#217. Discusses issues with electronic voting machines in the 2008 election cycle.

United States Election Assistance Commission, Voluntary Voting Systems Guidelines, http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx

United States Election Assistance Commission, Voter Systems Testing and Certification Program Manual (VSTCPM)
http://www.eac.gov/assets/1/Documents/Certification%20Program%20Manual.OMB%203265.004.Exp%206.30.2014.pdf (2011)

P.B. Stark, and D.A. Wagner. 2012. "Evidence-Based Elections." IEEE Security and Privacy. http://www.stat.berkeley.edu/~stark/Preprints/evidenceVote12.pdf. This source discusses the need for audit processes, with a focus on how to ensure the creation and preservation of evidence for ensuring the verifiability of election results. Argues that robust audit standards would reduce

costs by allowing for the relaxation of voting machine certification and testing standards.

Javed A. Aslam, Raluca A. Popa and Ronald L. Rivest, On Auditing elections When Precincts Have Different Sizes (2008), http://web.mit.edu/ralucap/www/AslamPopaRivest-OnAuditingElectionsWhenPrecinctsHaveDifferentSizes.pdf. Describes methods for auditing election results that reduce costs by varying sample size for precinct size.

Philip B. Stark, Conservative Statistical Post-Election Audits, 2 Ann. App. Stat. 550 (2008), http://www.stat.berkeley.edu/~stark/Preprints/conservativeElectionAudits07.pdf. Presents method for an escalating post-election audit. Previous methods asked only how to ensure finding an error if one existed (at a certain confidence level). This paper builds on those methods by answering the question of what to do once some miscounts are detected, and whether and when to confirm the outcome.

Pew Center on the States, "The Cost of Voting Technology" (2012) http://www.pewstates.org/research/analysis/the-cost-of-voting-technology-85899403212. Links to research in California, Maryland, North Carolina, Miami-Dade County, Florida, and Butler County, Ohio comparing costs of DRE vs. optical scan machines. "In each case implementing the optical scan technology has been estimated to be less costly." For example, "In 2010, researchers with the Research Triangle Institute found that using optical scan systems could save Maryland nearly $10 million. And in 2005 the Miami-Dade County elections office estimated the county could save more than $13 million over five years by switching from DREs to optical scan technology."

Brad Friedman, Diebold Voting Machines Can Be Hacked by Remote Control, Salon.com, (Sept. 27, 2011), http://www.salon.com/2011/09/27/votinghack/; Liebowitz, Matt, "It only takes $26 to hack a voting machine: Researchers demonstrated three different types of attacks," NBCNews.com (Sept. 28, 2011), http://www.nbcnews.com/id/44706301/ns/technology_and_science-security/t/it-only-takes-hack-voting-machine/#.UZ1I32RKmgp. These sources discuss attacks on Diebold DRE machines by researchers at Argonne National Laboratory. Video from the ANL group discussing the results can be seen at http://www.youtube.com/watch?v=DMw2dn6K1oI.

"Vulnerability Assessment Team (VAT): Election Security," Argonne National Laboratory, http://www.ne.anl.gov/capabilities/vat/election-security/. Discusses various security vulnerabilities and attacks, and overall security best practices for election systems.

Argonne National Laboratory Vulnerability Assessment Team, Suggestions for Better Election Security (2012), http://www.ne.anl.gov/capabilities/vat/pdfs/SuggestionsforBetterElectionSecurity.pdf. Summarizes common security mistakes found in voting systems, and makes recommendations for improved security of electronic voting

machines and processes used by election officials.

Blaze et al., Source Code Review of the Sequoia Voting System, California Secretary of State "Top-to-Bottom" Review (2007), http://www.sos.ca.gov/voting-systems/oversight/ttbr/sequoia-source-public-jul26.pdf

Andrew W. Appel et al., Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine, Princeton University Center for Information Technology Policy (2008), http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/voting/advantage/

Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine (2007), http://static.usenix.org/event/evt07/tech/full_papers/feldman/feldman_html/

Sharon B. Cohen, Auditing Technology for Electronic Voting Machines, Ph.D. Thesis, MIT, Caltech/MIT Voting Technology Project Working Paper #46 (2005), http://www.vote.caltech.edu/sites/default/files/vtp_wp46.pdf. Presents studies of user interactions with paper and audio audit trails for DRE machines. Participants found both audio and paper audits to be easy to use. Participants found more errors using the audio audit system, which took slightly longer to use (and was perceived as such). Participants strongly prefered paper to audio audit systems when asked to make recommendations for their county.

R. Michael Alvarez and Thad E. Hall, Electronic Elections : The Perils and Promises of Digital Democracy (2010). Discusses risks and tradeoffs of electronic voting, and argues, inter alia, for comprehensive risk assessment, holding all voting systems to the same usability, security, and auditability standards, focusing on risk management and mitigation, and developing collaboration for election security research across disciplines and between the private, public, and academic sectors.

Walter R. Mebane Jr., Election Forensics: The Second-Digit Benford's Law Test and Recent American Presidential Elections, in Election Fraud: Detecting and Deterring Electoral Manipulation (R. Michael Alvarez, Susan D. Hyde, and Thad E. Hall, eds.) (2008). Discusses methods for forensic detection of fraud in results. Extends Benford's law (a statistical pattern in occurrence of digits in measured data) as a signal for possible fraud, and analyzes results from elections in Florida in 2000 and 2004 and Ohio in 2004.