POST-ELECTION AUDITS: RESTORING TRUST IN ELECTIONS

Lawrence Norden, Aaron Burstein, Joseph Lorenzo Hall
and Margaret Chen

Brennan Center for Justice *at New York University School of Law*
and the
Samuelson Law, Technology & Public Policy Clinic
at the University of California, Berkeley School of Law (Boalt Hall)

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute that focuses on fundamental issues of democracy and justice. Our work ranges from voting rights to redistricting reform, from access to the courts to presidential power in the fight against terrorism. A singular institution – part think tank, part public interest law firm, part advocacy group – the Brennan Center combines scholarship, legislative and legal advocacy, and communications to win meaningful, measurable change in the public sector.

ABOUT THE SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC

The Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall) is the first clinic in the country to provide students with the opportunity to represent the public interest in cases and matters on the cutting-edge of high technology law. The Clinic provides a setting for law students to engage in research and advocacy projects with U.C. Berkeley graduate students from a wide variety of other disciplines. These teams allow students to identify and test research theories, cultivate interdisciplinary thinking about policy questions, and provide an opportunity to translate research findings into policy recommendations and advice. In so doing, the Clinic is training the next generation of lawyers and technologists working at the intersection of law, technology and public policy.

About the Authors

Lawrence Norden is Counsel with the Brennan Center's Democracy Program, working in the areas of voting technology, voting rights, and government accountability. He is the author of the just published *The Machinery of Democracy: Protecting Elections in an Electronic World* (Academy Chicago Publishers 2007) and a contributor to the Encyclopedia of American Civil Liberties (Routledge 2007). Mr. Norden leads the Brennan Center's research and advocacy on electronic voting systems and manages the Brennan Center's blog on New York State, ReformNY.blogspot.com. He is a graduate of the University of Chicago and New York University School of Law. Before joining the Brennan Center, Mr. Norden was in private practice, concentrating in commercial litigation, technology and bankruptcy law. He is admitted to practice in New York. He may be reached at lawrence.norden@nyu.edu

Aaron Burstein is the TRUST and ACCURATE Research Fellow for the Berkeley Center for Law and Technology and the Samuelson Law, Technology and Public Policy Clinic at the University of California, Berkeley School of Law (Boalt Hall). His current research includes examining how law and technology interact in several distinct areas, including electronic voting and computer and network security. Mr. Burstein holds a J.D. from Boalt Hall and was an attorney in the U.S. Department of Justice Antitrust Division in 2004-2006. He may be reached at aburstein@law.berkeley.edu.

Joseph Lorenzo Hall is a Ph.D. candidate at the University of California, Berkeley School of Information working under information law professors Pamela Samuelson and Deirdre Mulligan. Mr. Hall's academic focus is on mechanisms that promote transparency, as core functions of our government go digital. His Ph.D. thesis uses electronic voting as a critical case study in digital transparency. Mr. Hall holds master's degrees in astrophysics and information systems from U.C. Berkeley and is a founding member of the NSF CyberTrust ACCURATE Center (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections). He may be reached at joehall@berkeley.edu.

Margaret Chen is a Research Associate in the Democracy Program at the Brennan Center, working on voting rights and election reform. Prior to joining the Brennan Center, she was a paralegal at Paul, Weiss, Rifkind, Wharton & Garrison LLP. She also interned at the Office of the Manhattan Borough President C. Virginia Fields. Ms. Chen received her B.A. in economics and political science from Barnard College. She may be reached at margaret.chen@nyu.edu.

ACKNOWLEDGMENTS

The Brennan Center and the Samuelson Clinic thank Alex Yacoub, a student at New York University School of Law, for his substantial legal analysis, as well as his extensive review and edits of this paper. We also thank Policy Analyst Kahlil Williams and Research Associate Vijay Das of the Brennan Center, and Common Cause legal interns David Fialkov and Lindsay Frischer for their comments and research assistance. This paper benefited greatly from the insightful and thorough editorial assistance of Deborah Goldberg, Director of the Brennan Center's Democracy Program.

We are grateful to John McCarthy of the Verified Voting Foundation for his many helpful suggestions and ideas for improving this study. We thank David Jefferson, Chair of the California Post-Election Audit Standards Working Group and computer scientist at the Lawrence Livermore National Laboratory's Center for Applied Scientific Computing, and Robert Kibrick, Legislative Analyst at the Verified Voting Foundation for their careful review of drafts of this paper and substantive feedback. Pamela Smith, President of the Verified Voting Foundation was an indispensable resource with an extensive knowledge of state audit laws. We also thank Lee Mosher, Professor of Mathematics and Chair of the Department of Mathematics and Computer Science at Rutgers, the State University of New Jersey for his participation in conversations about post-election audits and this paper.

Common Cause and VotersUnite! created the chart on voting machine tally failures, which appears as Appendix A of this paper.

The participation of Aaron Burstein and Joseph Lorenzo Hall is made possible by the support of the National Science Foundation under A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), Grant Number CNS-0524745.

Generous grants to the Brennan Center from an anonymous donor, the Carnegie Corporation of New York, the Ford Foundation, the HKH Foundation, the JEHT Foundation, the Knight Foundation, the Open Society Institute, the Rockefeller Family Fund, and the Tides Foundation supported the development and publication of this paper. Opinions, findings, and conclusions or recommendations expressed in this paper are the responsibility solely of the authors and the Brennan Center.

AUDIT PANEL

The Brennan Center and the Samuelson Clinic convened a blue ribbon panel (the "Audit Panel") of statisticians, voting experts, computer scientists and several of the nation's leading election officials to assist them in reviewing and evaluating both existing post-election audit laws and procedures, as well as the papers of academics and election integrity activists who have frequently criticized such laws and procedures as inadequate. Based on input from the Audit Panel, the Brennan Center and Samuelson Clinic then made a number of conclusions and recommendations about best audit practices. These conclusions and recommendations are those of the authors alone, and should not necessarily be ascribed to audit panel members. The members of the Audit Panel are listed below*:

Kim Alexander, president and founder, California Voter Foundation

Georgette Asherman, independent statistical consultant, founder of Direct Effects

Ted Bromley, Legislation and Elections Administration, Connecticut Secretary of State

David Dill, Professor of Computer Science and Electrical Engineering, Stanford University

Mark Halvorson, Director, Citizens for Election Integrity Minnesota

S. Candice Hoke, Director, Center for Election Integrity, Cleveland State University

David Klein, Elections Research and Operations Specialist, Ohio Secretary of State

Michael Kozik, Managing Attorney, Legislation and Elections Administration, Connecticut Secretary of State

Lesley Mara, Administrative Office, Connecticut Secretary of State

Walter Mebane, Jr., Professor of Government, Cornell University

Marisa Morello, Administrative Office, Connecticut Secretary of State

Rene Peralta, PhD, former Research Scientist at Yale University Department of Computer Science

Ronald Rivest, Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

David Robin, Member, Chicago Bar Association Election Law Committee

Warren Slocum, Chief Elections Officer & Assessor-County Clerk-Recorder, San Mateo County, California

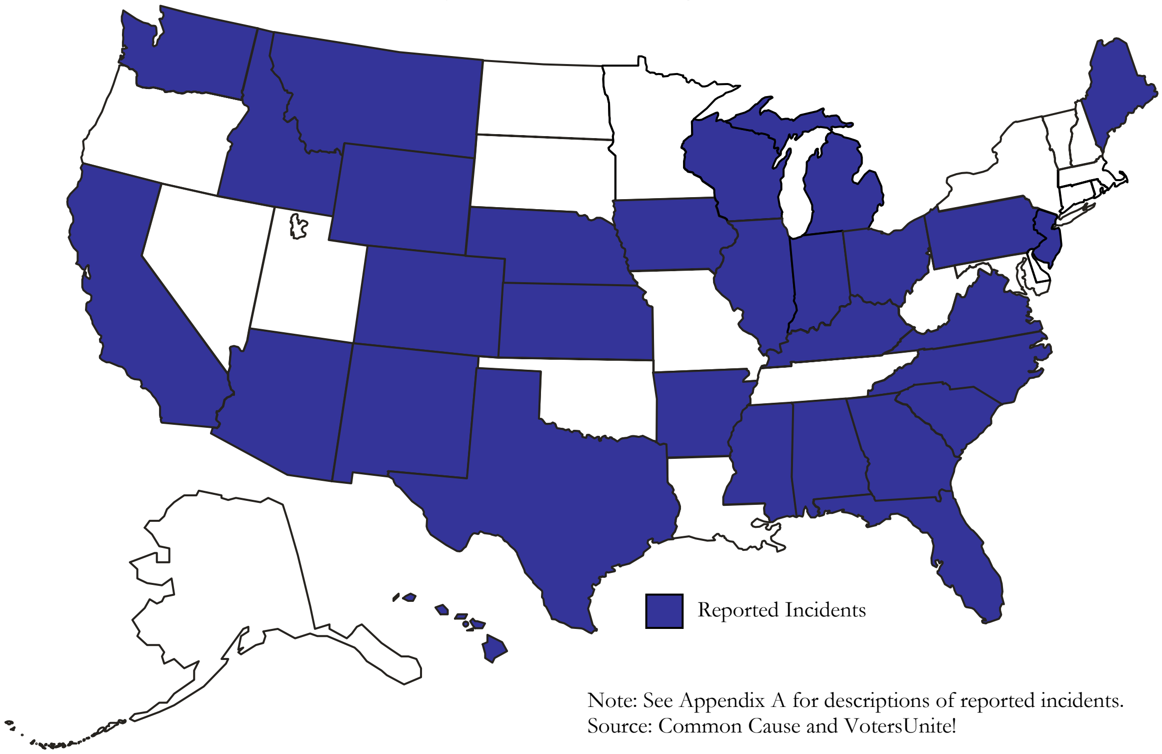
Anthony Stevens, Assistant Secretary of State, New Hampshire

David Wagner, Professor of Computer Science, University of California, Berkeley

*Organizational affiliations are shown for identification purposes only.

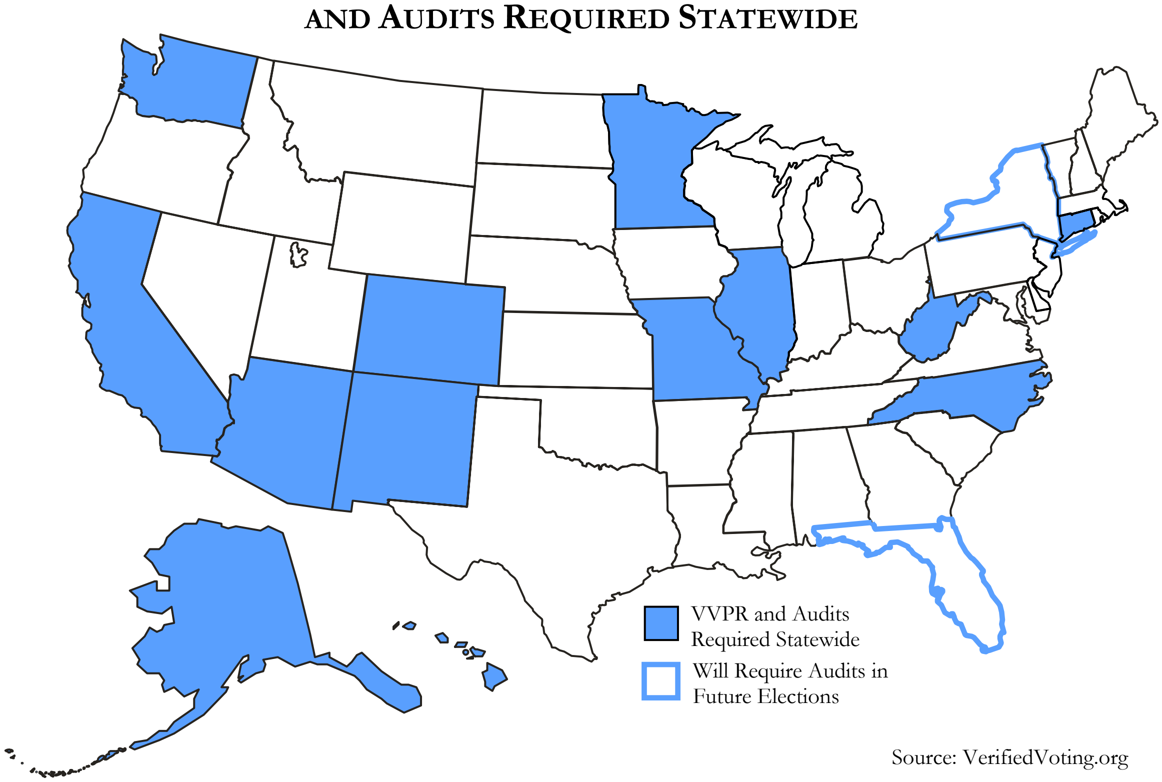
TABLE OF CONTENTS

FIGURE 1. REPORTED INACCURATE ELECTRONIC VOTE TALLIES AND MACHINE OUTPUT CAUSED BY SOFTWARE BUGS, PROGRAMMING ERRORS, AND OTHER FAILURES



Note: See Appendix A for descriptions of reported incidents.
Source: Common Cause and VotersUnite!

FIGURE 2. VOTER-VERIFIED PAPER RECORDS AND AUDITS REQUIRED STATEWIDE



Source: VerifiedVoting.org

I. INTRODUCTION

In the last several years, most of the public debate on electronic voting has concerned whether voting machines should include a voter-verifiable paper record. Today, in much of the country, that debate is over: thirty states require voter-verifiable paper records.[1] Another eight states use voter-verifiable paper records in every county without requiring them,[2] and of the remaining twelve states that do not use voter-verifiable paper records statewide, several are currently considering legislation that would mandate such records in the future.[3]

The widespread adoption of voter-verifiable paper records does not, however, resolve the security, reliability, and verifiability issues with electronic voting that many groups, including the Brennan Center, have identified. To the contrary, as the Brennan Center noted in its June 2006 comprehensive study of electronic voting system security *The Machinery of Democracy: Protecting Elections in an Electronic World*,[4] voter-verifiable paper records by themselves are "of questionable security value." Paper records will not prevent programming errors, software bugs or the introduction of malicious software into voting systems. If paper is to have any real security value, it must be used to check, or "audit," the voting system's electronic records.

Unfortunately, the purpose and value of voter-verifiable paper records has received scant attention and little study until recently. In the last year, statisticians and election integrity experts have appeared to make up for lost time, authoring and releasing dozens of separate papers about post-election audits of voter-verifiable paper records.[5] Meanwhile, the prospect of a federal requirement for post-election audits has galvanized many election officials and election integrity activists into publicly debating various audit methods and procedures.[6]

Much of the recent literature on post-election audits has been sharply critical of existing audit laws, regulations and practices.[7] However, many of these papers seem to contradict each other by promoting very different audit models, and very few provide practical advice about how to implement their recommendations to improve audit practices.

Sorting through this flood of often seemingly contradictory information and using it to improve post-election audits is no easy task. It is, however, critically important. In the next few months, Congress and several state legislatures are likely to consider and pass into law new post-election audit requirements, and the several states that already conduct post-election audits are considering amendments to existing audit laws and procedures.[8]

With the intention of assisting legislators, election officials and the public make sense of this new information and convert it into realistic audit practices, the Brennan Center and the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law (University of California Berkeley) convened a blue ribbon panel (the "Audit Panel") of statisticians, voting experts, computer scientists and several of the nation's leading election officials. Together with the Audit Panel, the Brennan Center and the Samuelson Clinic spent several months reviewing and evaluating both existing post-election audit laws and procedures, and the papers of academics and election integrity activists that have frequently criticized such laws and procedures as inadequate. Following this review and extensive consultation with the Audit Panel, the Brennan Center and the Samuelson Clinic make several practical recommendations for improving post-election audits, regardless of the audit method that a jurisdiction ultimately decides to adopt.

A. LIMITATIONS OF STUDY

We have limited our study to *post-election audits of voter-verifiable paper records*: how jurisdictions can use a randomly selected percentage of voter-verifiable paper records after the polls have closed to check the electronic vote tallies and the performance of electronic voting machines. There are many other types of examinations and audits of voting machines (and the entire voting system) that should be conducted before and after the polls close. For example, sound federal and state certification of voting systems, acceptance testing, and "logic and accuracy" testing are forms of pre-election audits and examinations that are critical to ensuring that voting systems accurately record and count votes. Similarly, after an election, comparisons of the number of ballots cast to the number of voters who signed in, interviews with poll workers, and full recounts of a contested election are important ways of adding transparency to elections and improving voting technology and election administration.

Instead of attempting to survey all of these elements of examination and auditing, we have chosen to focus on voter-verifiable record-based audits of electronic vote tallies because these audits are at the center of many current legislative debates over election integrity, and because they hold immediate and long-term value for election integrity. The kinds of post-election audits that we discuss here may lend confidence in the results of a close election as well as shed light on voting system problems even when elections are not close. Although it would be ideal to detect voting system problems before an election takes place, the past few elections have shown that some problems may be unavoidable, irrespective of the precautions that election officials take. This report sets forth ways in which post-election audits using voter-verifiable paper records may nevertheless provide a systematic means of understanding voting system performance (and failures).

B. SUMMARY OF FINDINGS

Our study of the current academic literature and current state audit laws and procedures points to several important findings:

- Post-election audits of voter-verifiable paper records are a critical tool for detecting ballot-counting errors, discouraging fraud, and improving the security and reliability of electronic voting machines in future elections. Unfortunately, of the thirty-eight states that require or use voter-verifiable paper records throughout the state, twenty-three do not require such audits after every election.[9]

- Of the few states that currently require and conduct post-election audits, none has adopted audit models that will maximize the likelihood of finding clever and targeted software-based attacks, non-systemic programming errors, and software bugs that could change the outcome of an election.

- We are aware of only one state, North Carolina, that has collected and made public the most significant data from post-election audits for the purpose of improving future elections. Based upon our review of state laws and interviews with state election officials, we have concluded that the vast majority of states conducting audits are not using them in a way that will maximize their ability to improve elections in the future.

- Regardless of the audit model a jurisdiction implements, there are several simple, practical, and inexpensive procedures that it can adopt to achieve the most important post-election auditing goals, without imposing unnecessary burdens on election officials.

C. Post-Election Audit Considerations

In our analysis of the post-election audit debate, we found that much of the disagreement about what constitutes a "sound" audit actually centers on disagreement over the *purpose* of an audit. In fact, there are a number of goals that a post-election audit may serve, and by emphasizing one, jurisdictions may make it more difficult to fulfill another. Among the goals an audit can fulfill are:

- creating an appropriate level of public confidence in the results of an election;

- deterring fraud against the voting system;

- detecting and providing information about large-scale, systemic errors;

- providing feedback that will allow jurisdictions to improve voting technology and election administration in future years;

- providing additional incentives and benchmarks for elections staff to reach higher standards of accuracy;[10] and

- confirming, to a high level of confidence, that a complete manual recount would not change the outcome of the race.[11]

This paper is the first to articulate all of these goals and to comprehensively examine the trade-offs that may be entailed to satisfy all of them. We also look at additional factors that jurisdictions will probably want to consider when developing audit methods and procedures, including to what extent the audits will be administratively burdensome (i.e., how much they will cost, how many hours they will take to complete, and how much certainty a jurisdiction will have about these issues prior to Election Day) and whether their effectiveness will depend heavily on the subjective judgments of election and other public officials in charge of the audit (something jurisdictions should generally want to avoid).

In most cases, lower administrative costs and greater certainty about the audit ahead of time means less certainty that evidence of an outcome-changing error or of fraud will be found once the election is over. Similarly, audits that are efficient at detecting widely distributed, systemic errors can provide feedback to improve elections, but are often poorer at pinpointing errors that might have affected the outcome of an election. They also generally provide election officials with little guidance as to what should be done when discrepancies between the paper and electronic records are found.

D. SUMMARY OF AUDIT RECOMMENDATIONS

We do not endorse any particular audit model as the "best" one. Instead, we have identified certain basic principles that all jurisdictions should adopt, regardless of the audit model they choose. These recommendations are based on consultation with the Audit Panel and a thorough review of current practices in states and counties where audits are conducted, as well as recent academic literature on post-election audits. The recommendations can be broken into three categories: (1) best practices for selecting votes to be audited; (2) best practices for conducting the audit itself; and (3) best practices for ensuring audit effectiveness. They are discussed in much greater detail in "Audit Best Practices" *infra* at page 30 (additional recommendations for specific models are discussed in "A Review of Current and Proposed Audit Models" *infra* at page 9).

SELECTING VOTES TO BE AUDITED

The method and manner employed by a jurisdiction for choosing votes to audit will have a tremendous impact on whether the audit itself is administratively burdensome, engenders public confidence in election results, detects errors, and provides feedback that will allow jurisdictions to improve elections in the future. Among the most important steps that jurisdictions can take in selecting votes to be audited are the following:

- **Use Transparent and Random Selection Processes for All Auditing Procedures.** Audits are more likely to prevent fraud and produce greater voter confidence in election results if the public can verify that the paper records, machines, or precincts to be audited are chosen in a truly random manner.

- **Consider Selecting Precincts or Machines for Auditing at the State Level.** While there are some disadvantages to centrally-conducted audit selection (discussed *infra* at page 32), there are many benefits for election officials to consider, including efficiency, transparency, and standardized procedures. By choosing precincts or machines to audit at the state level, counties are relieved of this responsibility and associated administrative tasks. Additionally, audit selection at the state level facilitates the selection of precincts to audit in election districts that cross jurisdictional boundaries. Finally, public observers of random selection processes would be able to watch a single selection process, rather than attempt to watch multiple county selection processes around a state.

- **Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.** Much of the recent academic literature on post-election audits focuses on catching error or fraud that could change the outcome of an election. But finding an error that has changed the outcome of an election is in many ways a worst case scenario; most would prefer finding and correcting such errors in landslide elections where they could not affect the outcome. An audit of a minimum number of precincts or machines supports election officials' efforts to monitor overall voting system performance and ensure that the machines operate optimally.

- **Account for Precinct Size Variability in Audit Selection and Sample Size Calculations.** Any procedures that do not take into account the varying number of votes in different precincts are likely to overestimate the audit's confidence level (or "statistical power") with respect to uncovering irregularities that could change the outcome of an election. Methods to deal with precinct size variability can be as simple as sorting precincts into bins of certain sizes (e.g., "small," "medium," and "large") and conducting random selection within each bin, or listing precincts in order of size and ensuring that auditors select a certain number of large precincts.

- **Allow Candidates To Select Precincts or Machines To Be Audited.** Making this option available to candidates would serve two purposes. First, it would give greater assurance to candidates and their supporters that that the election results are correct. Second, it would allow candidates to prompt audits of seemingly anomalous results that could suggest a programming error or miscount.

CONDUCTING THE AUDIT

There are specific steps that every jurisdiction can take to make it far more likely that the audit is accurate, useful to election officials, and likely to catch errors that could change the outcome of certain races. Most importantly, jurisdictions should:

- **Freeze and Publish Unofficial Election Results Before Selecting Precincts or Machines to be Audited.** Election officials should freeze and publish unofficial election results once all returns are received from jurisdictions. The random selection of precincts or machines to be audited should only occur afterwards. This practice allows the public to verify the accuracy and fairness of audit results.

- **Conduct "Blind" Manual Counts.** While unofficial totals should be made available to the public so that they can verify the accuracy and fairness of the audit, manual counters should be "blind" to the unofficial election results for the machines they are auditing to ensure that knowledge of the unofficial results does not influence their counting.

- **Don't Just Match – Count! (Record and Publicly Release Meaningful Data on Votes Cast).** Audits that record and detail the overvotes, undervotes, blank votes, spoiled ballots, and, in the case of DREs, cancellations, could be extremely helpful in revealing software attacks and software bugs and in identifying problems with ballot design and/or ballot instructions. Rather than only matching paper and electronic tallies, election officials should record and publicly release this meaningful data, which should be useful for improving elections in the future.

- **Consider Auditing by Machine Rather Than Precinct.** In many states, it will be more efficient to audit by machine or ballot batches rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same level of confidence in their results by auditing a smaller percentage of machines.

- **Audit All Methods of Voting.** In conducting post-election audits, election officials should not exclude any category of votes (e.g., absentee ballots, provisional ballots, damaged ballots). In 2004, seven states reported that more than twenty percent of all votes were cast during early voting periods.[12] Excluding these ballots from an audit would leave a significant opportunity for errors to remain undetected.

ENSURING OVERALL AUDIT EFFECTIVENESS

If the audit is to be effective, jurisdictions must have certain basic policies and practices in place. Principally, jurisdictions ought to:

- **Ensure the Physical Security of Audit Materials.** Effective auditing of voter-verifiable paper records will serve to deter attacks on voting systems and identify problems only if states have implemented solid procedures to ensure the physical security of election materials used in a post-election audit, including the paper records of the vote, voting machines, and tally servers.

- **Implement Effective Procedures for Addressing Evidence of Fraud or Error.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing discrepancies between the paper records and electronic tallies when they are found. Without protocols for responding to discrepancies, the detection of fraud or error will not prevent it from successfully altering the outcome of an election. Recommended responses include making corrections where warranted, disallowing results if an appropriate remedy cannot be determined, and ensuring accountability for discrepancies. Jurisdictions should document discrepancies and any actions in response to them in publicly available discrepancy logs.

  When there have been no losses or additions of paper records, a single unexplained discrepancy between the paper records and electronic tallies is a strong indication of a software problem of some kind. Any such discrepancy, even if it is just one vote and can have no effect on the outcome, is grounds for a review of voting machine software code. Such a review need not delay certification of the election, but it should be investigated. To be effective, election officials must have the ability to audit the code, not just the votes.

- **Audit the Entire Voting System, Not Just the Machines.** Although this study focuses only on post-election audits of voter-verifiable paper records, jurisdictions should conduct audits of the entire voting system to catch errors or fraud in other parts of the voting system. Historically, incorrect vote totals often result from aggregation mistakes at central vote tally locations. Accordingly, good audit protocols will mandate that the entire system – from early and absentee ballots to aggregation at the tally server – be audited for accuracy. This should also include, at the very least, the ability of election officials to audit the code where they deem necessary.

II. A REVIEW OF CURRENT AND PROPOSED AUDIT MODELS

There are three basic categories of post-election audits described in current law, proposed bills, and academic literature. They are as follows:

A. **Fixed-Percentage Audit Model.** In this model, jurisdictions are required to randomly select a fixed percentage of precincts or machines to audit. All voter-verifiable paper records for the selected precincts or machines are hand-counted and compared to the electronic tallies. Most states that currently conduct post-election audits embrace this model.

B. **Adjustable-Percentage Audit Model**. This model requires jurisdictions to determine the percentage of precincts or machines to audit based on the size of the margin of victory between the two leading candidates in a race. The smaller the margin of victory, the larger the percentage of precincts or machines to audit. While we are unaware of any state that has explicitly adopted a form of this audit model, several states require full or partial recounts of voter-verifiable paper records when races are extremely close.[13] Moreover, most of the recent academic articles we have reviewed have endorsed this method, and it appears to be gaining support among legislators and election integrity activists around the country.[14]

C. **Polling Audit Model.** This model requires a randomly chosen, small sample of ballots be recounted in *every* precinct and that these tallies be compared to the unofficial electronic results. We are not aware of any jurisdictions that have adopted this approach, though several election integrity advocates have endorsed it.[15]

In the subsections below, we describe and evaluate each audit model in detail and provide specific recommendations (in addition to those already discussed *supra* at 5–8) for improving each one.

A. THE FIXED-PERCENTAGE AUDIT MODEL

This model, embraced by most states that currently conduct audits, requires jurisdictions to randomly select a fixed percentage or a fixed number of precincts or machines to audit. All voter-verifiable paper records for the selected precincts or machines are manually counted and compared to the electronic vote tallies.

1. MODEL IMPLEMENTATION

Because some variant of this audit model is used in at least fourteen states, we have several examples of how it can be implemented.

The minimum fixed audit percentages have ranged from Utah's audits of one percent of voting machines to Connecticut's recent audit of twenty percent of precincts using optical scan voting machines.[16] There is a considerable range between these extremes, though most states tend to fall at the lower end of the spectrum. Aside from Hawaii, which requires an audit of ten percent of precincts, the other states that have adopted the **fixed-percentage** approach require minimum audits of five percent of precincts or machines, or less.[17] In Minnesota, rather than specifying a percentage, the number of precincts to audit in each county depends on the number of registered voters: counties with fewer than 50,000 registered voters must audit at least two precincts, while counties with more than 100,000 registered voters must audit at least four precincts.[18]

States also differ on the question of whether to audit precincts or individual voting machines. The basic principle in both cases is the same: auditors must tally paper records and compare the results to the electronic tally for the recounted precinct or machine. For the reasons explained by Howard Stanislevic in a paper on determining the proper size of an audit,[19] a machine-level audit can produce the same confidence level as a precinct-level audit with a lower amount of effort. (Alternatively, for the same level of effort, a machine-level audit can produce a higher confidence level than a precinct-level audit.) Most states that conduct **fixed-percentage** audits do so at the precinct-level, though New York plans to conduct manual audits at the machine-level.[20]

Another variable among these states is the number of contests reviewed in an audit. Connecticut, California, and Illinois check all of the races on a ballot during a post-election audit, which in California, can be as many as 200 races.[21] In contrast, both Hawaii and New Mexico review just one race in an election during a post-election audit.[22] Arizona requires jurisdictions to review at least 4 contested races, including one federal race, one statewide race, one ballot measure, and one legislative race.[23]

Finally, states vary in how they select the precincts or machines to be audited. In California, for instance, precincts are chosen at the county level, with little direction from the state as to how the precincts should be selected.[24] By contrast, precincts are selected at the state level in Illinois.[25]

As discussed *infra* at page 32, centralized audit selection can be more efficient and transparent. By selecting precincts or machines to audit at the state level, counties are relieved of this responsibility and associated administrative tasks. Additionally, audit selection at the state level facilitates the selection of precincts to audit in election districts that cross jurisdictional boundaries. Finally, public observers of random selection processes would be able to watch a single selection process, rather than attempt to watch multiple county selection processes around a state.

State-level audit selection, however, carries some disadvantages. Some states may be too large – geographically, or in terms of the number of precincts, or both – to select precincts in a reasonable amount of time during a single official event. Selecting precincts or machines to audit in a central location might also make it difficult for local election officials and voters to observe the selection process for their own jurisdiction. This could undermine the transparency that public audit selection should foster. Finally, since audit selections should occur after all ballot types, including absentee and provisional ballots, have been counted, there is a risk that a single jurisdiction with a high proportion of these could hold up statewide audit selection.

Regardless of whether a jurisdiction chooses to audit by precinct or machine, audit one percent or twenty percent, or select precincts or machines at the state or county level, there are certain procedures that must be implemented if this model is to be as effective and efficient as possible. We discuss some of these procedures below.

2. AUDIT MODEL STRENGTHS

The **fixed-percentage** audit model should detect errors and fraud above a certain threshold (dependent on the size of the audit). Assuming a low, single-digit percentage audit, this type of audit should easily detect a software bug or programming error that affects large numbers of votes on a large number of machines.

Moreover, when an unexplained discrepancy between the paper records and electronic tallies is found, it should be fairly easy for election officials to identify the machine, race and/or ballot type affected by the discrepancy. Thus, we can imagine a scenario where a software bug on certain DREs causes the machines to lose the electronic record of anyone who has voted on Spanish language ballots. The direct comparison of paper records (which have not been lost) to electronic tallies should allow us to identify fairly quickly which types of ballots have been affected. As discussed in greater detail below, this is not necessarily true of other audit methods (see *infra* at page 28).

Finally, under this audit model, jurisdictions will have comparatively low and foreseeable administrative costs. Because jurisdictions know in advance what percentage of precincts or machines will be audited, they may make the necessary logistical preparations for a post-election audit, such as hiring auditors and determining how long the audits are likely to take.[26]

3. AUDIT MODEL WEAKNESSES

While the **fixed-percentage** audit model has the benefits of detecting widespread discrepancies, yielding detailed information about their possible sources, and of imposing predictable costs and time requirements, it has two major weaknesses. The first weakness has been identified in several academic papers: the closer a race is, the less likely this type of audit can provide confidence that a software bug, programming error, or malicious software attack did not alter the outcome of the election.[27]

As an example of this first weakness, Table 1 illustrates the problem of low confidence levels in a typical Congressional district of 400 precincts which are assumed to be of roughly equal size for the purposes of simplicity. We have assumed that this state mandates an audit of five percent of all precincts (as is the case, for example, in Illinois). We have further assumed that if more than twenty percent of the ballots in any single jurisdiction were corrupted, election officials and the public would detect the corruption without an audit. This is a common assumption in academic literature on post-election audits.[28]

TABLE 1. FIXED-PERCENTAGE AUDIT OF FIVE PERCENT OF PRECINCTS IN THE MODEL CONGRESSIONAL DISTRICT

No. of Precincts	Margin of Victory	Confidence Level
400	5%	94%
400	2%	65%
400	1%	40%

Note: If a Congressional District has fewer than 400 precincts, confidence levels will be significantly lower. If precinct size varies within a Congressional District, it will be more difficult to obtain a high level of confidence in the results, unless precinct selection is weighted by the number of voters in each precinct.[29] Weighted precinct sampling is discussed in greater detail *infra* at page 25.

The numbers in Table 1 were calculated assuming a two-person race, where "margin of victory" is determined by subtracting the total votes for the loser from the total votes for the winner, and dividing by the total number of ballots cast and counted. The smaller the margin of victory, the less confidence we have that the five percent audit will catch a software bug, programming error, or malicious software attack that could have altered the results of an election. The reason for this is simple: in a race decided by more than five percent of the vote, a software bug, malicious attack, or programming error will have to affect a large number of votes to change the outcome of the election. A five percent audit should catch such an error that affects a large number of votes. In contrast, in a race decided by only one percent of the votes, a software bug, malicious attack, or programming error will only have to corrupt a small number of votes to change the outcome. In this case, there is a small chance that we would find the corrupt machines or precincts if we audited only five percent of them.

In the discussion above, we have assumed that the Congressional district in question is contained within a single election jurisdiction. In practice, many Congressional districts span multiple counties, which are, in turn, responsible for administering their own elections. In such cases, counties will be sampling from an even smaller number of precincts than a jurisdiction would sample if it selected from the entire Congressional district, without regard to county borders. Sampling a fixed percentage of this smaller (county-based) number of precincts will produce an even lower confidence level than the numbers discussed above.

ADDRESSING THE PROBLEM OF LOW CONFIDENCE LEVELS

Princeton University Professor Andrew Appel and others have proposed a remedy to the problem of low confidence levels produced by a **fixed-percentage** audit: allow candidates to select additional precincts or machines to be audited.[30] This practice of non-random and "targeted" auditing is common in the financial industry and other areas where government has an interest in ensuring honest reporting.[31] It is already effectively enshrined in law in some states, such as New Hampshire and North Dakota, where candidates can ask for recounts in some or all precincts at little or no cost.[32]

We endorse this suggestion for all elections, as it would serve two confidence-building purposes. First, it would give greater assurance to candidates and their supporters that the election results are correct. Second, it would allow candidates to receive audits of results that seem anomalous and might suggest a programming error or miscount. Given the low confidence levels produced by **fixed-percentage** audits of close elections, this recommendation is particularly important.

Another potential remedy to this weakness would be to increase the level of audits in very close races. Several states that conduct **fixed-percentage** audits require a full recount of paper records when the margin of victory between the two leading candidates is very small. Connecticut automatically requires a recanvass of voting machine returns and absentee ballots if the margin of victory between the top two candidates is less than twenty votes or less than one half of one percent of the total votes cast for the office in question (up to 2,000 votes).[33] In Arizona, if the margin between the two top candidates is equal to or less than one tenth of one percent of the number of votes cast for both candidates, a full recount for the affected office will occur.[34] How to implement this remedy is discussed in greater detail in the next section of this paper "The Adjustable-Percentage Audit Model" *infra* at page 19.

ACTING ON DISCREPANCIES

The second weakness of the **fixed-percentage** audit model is that discrepancies that may seem minor (e.g., a three-vote discrepancy between the paper records and electronic tallies in a particular precinct) could indicate far larger problems. This model will be effective only if investigations and additional action are initiated when discrepancies between the paper records and electronic tallies are found.

The discovery of any discrepancy should prompt two actions. First, additional manual counts should occur to confirm the existence of discrepancies. Of the states that have laws or regulations relating to audit discrepancies, only eight require additional audits when such discrepancies are discovered, and those requirements for further action vary widely.[35] Hawaii audit law requires additional auditing if discrepancies are found, but does not describe how the additional auditing should be conducted.[36] In Minnesota, a difference greater than one half of one percent between the result of a manual audit and the electronic tally triggers the auditing of at least three additional precincts in the affected jurisdiction. If the discrepancy persists, the county auditor must review ballots in the rest of the county.[37] In New Mexico, a difference between the manual count and electronic tally greater than one and one half percent triggers a recount of ballots cast for the affected office in the legislative district where the discrepancy occurred.[38] In Arizona, discrepancies between the paper records and the electronic vote tallies equal to or greater than a "designated margin" trigger a second manual count. If after a second manual count discrepancies equal to or greater than the accepted "designated margin" persist, the audit is expanded to include twice as many precincts, randomly selected by lot.[39]

Some discrepancies between paper and electronic counts may be caused by human counting errors or by different interpretations of voter intent by a human counter and a voting machine. Although discrepancies are not necessarily proof that there was widespread fraud or error, as the Brennan Center Task Force on Voting System Security noted in *The Machinery of Democracy*, they can indicate a much larger problem with the election.[40] As such indicators, discrepancies should trigger other types of action by election officials.

Our second recommendation for acting on discrepancies is to investigate their causes and to respond appropriately to investigation findings.[41] For example, in Minnesota, if a voting system is found to have failed to record votes accurately and in the manner provided by the Minnesota election law, the voting system must not be used at another election until it has been examined and recertified by the Secretary of State. If the voting system failure is attributable to either its design or to actions of the vendor, the vendor must forfeit the vendor bond and the performance bond as required by Minnesota law.[42]

Generally, our review of state laws and interviews with election officials revealed that the majority of jurisdictions do not have adequate, detailed, and practical procedures for action to be taken when unexplained discrepancies are found. Jurisdictions should conduct a transparent investigation of all machines where the paper records and electronic tallies do not match to try to determine the cause of any discrepancies. In particular, especially for DREs, an investigation should include a review of the software code, as discrepancies may have been caused by a software bug or programming error. As in Illinois, the "State Board of Elections, State's Attorney and other appropriate law enforcement agencies, the county leader of each political party, and qualified civic organizations" should be notified of the discrepancies and have an opportunity to send observers to the investigation.[43] Additionally, election officials should create a "discrepancy log" in which to list all discrepancies, identify the precinct and machine where they occurred, describe their causes, and record any actions taken in response to them. The discrepancy log and the findings of any investigation should be made available to the public. The adoption of these two practices would significantly strengthen the **fixed-percentage** audit model's ability to serve as an effective countermeasure to outcome-changing fraud or error.

4. ADMINISTRATIVE CONSIDERATIONS

TIME AND COST OF AUDIT

Because the number of precincts or machines audited rarely changes significantly from one election to the next, the time and cost of **fixed-percentage** audits should remain stable over time. These factors should only change significantly if discrepancies trigger additional audits. Determinants of the time and cost of an audit include: the percentage of precincts or machines audited, the number of persons staffing the audit, and the number of races audited.

State reporting of the amount of time it takes to complete an audit varies. Counties in Illinois report that five percent audits of ten to twelve races in an election generally take anywhere between two hours to two days.[44] In Hawaii, an audit of ten percent of precincts for a single race is generally completed in less than a week.[45] In Clark County, Nevada, where officials audited dozens of races in two percent of precincts in 2006, the audit was completed in just a few days.[46] In Los Angeles County, California, it has generally taken close to twenty-eight days to select and audit one percent of all of the contests in a general election (since 2000, that number has been anywhere between 134 and 194 contests).[47]

The largest component of a **fixed-percentage** audit's cost is likely to be associated with managing and staffing the audit. If states hope to achieve accurate audit results using best practices applied consistently, the preponderance of the costs of audits is likely to lie in recruiting, paying, and training quality management and covering travel costs – at least in initial years. These costs will vary, depending on the number of auditors required to complete the audit and the magnitude of any financial compensation. During Hawaii's ten percent audit of a single race in 2006, the smallest county required seven auditors while the largest county required forty-five.[48] In many cases, jurisdictions use election workers already on their payroll to avoid incurring additional staffing costs.[49] A typical hand count on election night in 2006 in Walpole, New Hampshire involved nine two-person teams and three managers to count 1,574 ballots, with each ballot having the equivalent of 14 contests.[50]

Despite this variance, for all cases where we have been able to review actual cost data, the overall cost of a **fixed-percentage** audit has been surprisingly low compared to what is already spent by jurisdictions on elections. Unfortunately, comparing the costs of one jurisdiction to the next is difficult because jurisdictions report costs differently, some on a per ballot basis and others on a per precinct basis. In North Carolina's first audit in 2006, the average cost of the audit of a single race in 260 precincts was sixty-five dollars per precinct.[51] In November 2006, Minnesota examined three contests in 202 precincts at an estimated cost of $135 per precinct.[52] Pima County, Arizona examined four contests in each of nine precincts, plus additional provisional ballots, for a little over thirteen cents per ballot.[53] Had they paid the market rate of $7-10 per hour for counters and $20 per hour for managers, the 2006 Walpole, New Hampshire election night hand count of 1,574 fourteen-race ballots, with nine two-person counting teams, would cost about four cents per ballot, per race.[54]

THE CHALLENGE OF MATCHING PAPER AND ELECTRONIC RECORDS

Counting paper records presents at least two related problems. The first is that people often miscount. Consequently, there are going to be many instances where the hand count of paper records and the electronic tally do not match, not because there was a problem with the machines, but because the auditors made mistakes counting. There has been very little research evaluating different methods of hand-counting, but we discuss directions such research should take in the "Directions for the Future" section of this paper *infra* at page 40.

Several jurisdictions partially address the problem of miscounting by having at least two people count the same paper record.[55] For example, San Mateo County, California uses a team of four people to conduct their post-election audit.[56] One person reads and announces the contents of a given paper record, another observes that the paper record has been announced correctly and two people record a running tally of votes for each contest. The recorders announce the end of each ten-vote increment, at which point the team checks for errors in the tally. If the team finds an error, the counting process can be rolled back to the last point of agreement.[57]

Minnesota provides an example of how incremental checking during post-election audits works in practice. Minnesota law requires election judges to count the votes for each race or ballot question by creating piles of voted ballots for each candidate in a race and piles for blank or defective responses.[58] Election judges check the sorted piles of ballots for the particular race or question to ensure that all ballots have been placed in the correct pile. Ballots may be stacked in groups of twenty-five crosswise.[59] After the final count for the race or question is completed, all ballots are returned to a single pile and the process is repeated for the subsequent race or ballot question.

The second, related problem is that auditors are likely to *want* the paper records to match the electronic records. The problems in Cuyahoga County, Ohio in 2004, where audit supervisors rigged the ballot selection so that no discrepancies would be found, exemplify the danger of auditors hoping to find perfect matches and to avoid the difficult questions and additional work that might result if the records do not match.[60]

To counter the understandable temptation to make the paper and electronic records match, we recommend against revealing the unofficial electronic election results to the individuals performing the manual count. The audit teams should not have access to the unofficial results; an audit supervisor or election official can serve as a buffer and inform each team if their audit results match the unofficial electronic results, without revealing the magnitude or direction of any deviation. If the manual count does not match the electronic results, the audit team should conduct additional "blind" recounts of the records of affected races.[61] This practice need not prevent elections officials from freezing and publishing unofficial election results prior to conducting the audits; it merely means that auditors should not be made aware of the vote tallies on the particular machines they are auditing.

Manual counts may sometimes reveal different voter intent than machine counts of ballots. Overvotes, marginal marks, hesitation marks, and other stray markings on manually marked ballots could cause optical scan voting machines to misinterpret voter intent that a human reviewer would be able to discern. This may lead to deviations or explained discrepancies when auditing optical scan paper ballots. Fortunately, these discrepancies are easy to recognize and account for, so they should not cause any serious problem; they qualify as an explained discrepancy and need not trigger any kind of recount or additional audit, except in the case of an extremely close race.

OTHER FACTORS

Jurisdictions that use DREs with voter-verifiable paper records may face an extra challenge in sorting paper records by precinct prior to auditing, creating additional costs. Some jurisdictions locate precincts with different ballots in a single polling place. Voting machines in a polling place may be programmed to store and enable multiple precinct ballot layouts, allowing voters of different precincts to cast ballots on a single machine. As a result, the polling place's set of voter-verifiable paper records will need to be carefully sorted by precinct so that the records for a precinct selected for auditing will not include records corresponding to other precincts. Alternatively, if a precinct in a multiple-precinct polling place is selected for an audit, election officials can automatically add the other precincts in the polling place to the audit to avoid the costs of sorting records.

An additional consideration for all audit methods is the quality of the voter-verifiable paper records. A widely reported problem with the current generation of DREs outfitted with voter-verifiable paper record printers is that some of the records are unreadable. For example, in Cuyahoga County, Ohio's May 2006 primary election, ten percent of the paper records were unreadable due to paper jams and other printer malfunctions.[62] A high proportion of spoiled voter-verifiable paper records could have significant negative consequences on an audit's effectiveness. Quantifying the impact of spoiled paper records is beyond the scope of this paper, but a qualitative example might be helpful. Spoiled paper records could effectively hide discrepancies and thus allow a greater proportion of discrepancies per precinct to go undetected. For an **adjustable-percentage** audit (discussed *infra* at page 19), this would lead to an underestimate of the audit size. More generally, spoiled voter-verifiable paper records could drown out the effect of more subtle voting system errors, frustrating the goal of collecting data about voting machine performance during audits.

5. RECOMMENDATIONS TO IMPROVE THE MODEL

In addition to the general recommendations for all audit models made in the "Audit Best Practices" section on page 30 and which we strongly reiterate here, we also make the following recommendation to strengthen the **fixed-percentage** model:

- **Implement Effective Procedures for Acting on Seemingly Small Discrepancies.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing audit discrepancies when they are found. As noted in *The Machinery of Democracy*, a seemingly minor discrepancy between paper and electronic records (of even just a few votes) could indicate far more serious problems.[63] Without protocols for responding to discrepancies, the detection of fraud or error will not prevent them from occurring again. Such protocols should include a required review of system software code.

Furthermore, given the low-confidence levels that a **fixed-percentage** audit will sometimes produce, we highlight the following recommendation for the fixed-percentage model in particular:

- **Allow Candidates To Select Precincts or Machines To Be Audited.** In addition to using random selection procedures, jurisdictions should allow candidates to pick at least one precinct or machine to be audited. This practice would allow candidates to receive audits of results that seem anomalous to them and give greater assurance that the election results are correct.

B. THE ADJUSTABLE-PERCENTAGE AUDIT MODEL

The **adjustable-percentage** audit model attempts to address the problem of low confidence levels in close races produced by the **fixed-percentage** audit model. This audit model requires a state or local jurisdiction to determine what percentage of precincts or machines to audit for each race based on the size of the margin of victory between the two leading candidates. The smaller the margin of victory, the larger the percentage of precincts or machines that will need to be audited. The mathematics behind this method involves calculating a sample size given the margin in the closest race on the ballot and a desired confidence level for detecting error or fraud.[64]

Many recent academic articles endorse variants of the **adjustable-percentage** audit model – often in conjunction with adjustments for variations in number of voters in different units (e.g., precincts or machines) – and it appears to be gaining currency among legislators and election integrity activists around the country.[65] Congressman Rush Holt proposed a variation of the **adjustable-percentage** audit model in the "Voter Confidence and Increased Accessibility Act of 2007," which currently has support from more than a majority in the U.S. House of Representatives.[66] Legislators and chief election officials in several states are also considering adoption of similar audit methods.

1. MODEL IMPLEMENTATION

The goal of an **adjustable-percentage** audit is to reach a minimum level of "confidence." In this context, confidence refers to a measure of the probability that a full recount of the voter-verifiable paper records would not change the outcome of an election. To make this determination, a jurisdiction will need to know a few things: the number of precincts or machines to be audited, the variation in the number of votes per precinct or machine, the unofficial margin of victory, and the confidence level or "statistical power" the jurisdiction would like to achieve.[67]

With this information and the use of scientifically reasonable assumptions (discussed in detail below at page 20), election officials (with the assistance of statisticians, where necessary) can determine how many precincts or machines to audit to reach a desired minimum level of confidence. To illustrate this more concretely, consider the meaning of an **adjustable-percentage** audit that yields a ninety-five percent confidence level: holding the assumptions discussed below as true, if an outcome-changing level of error or fraud exists, there is a ninety-five percent chance that this audit will detect it (and, accordingly, a five percent chance that it will not). An audit designed to give a fifty percent confidence level would have an equal chance of finding and not finding such error or fraud.

An **adjustable-percentage** audit can be implemented in several different ways. We discuss two of the most commonly suggested methods below.

AUDITS OF ADDITIONAL PRECINCTS OR MACHINES IN CLOSE RACES

One implementation of the **adjustable-percentage** audit model is similar to the implementation of the **fixed-percentage** audit model discussed earlier. If a state requires an audit of a minimum percentage of precincts or machines, selection can begin at the state or county level as soon as the unofficial results are frozen and published. For any close races, election officials will select additional precincts to audit to achieve a desired level of confidence. We note that many states that currently have **fixed-percentage** audit laws specify a minimum percentage to be audited, and could implement **adjustable-percentage** audits without running afoul of these laws.

The determination of how many additional precincts to select in close races (and their subsequent selection mechanism) is a challenge that is unique to this model. We examine below how a state-level entity could select additional precincts in federal races with small margins of victory. We discuss this arrangement, which deviates from most states' county (or other jurisdiction)-based procedures for two reasons. First, a centralized procedure may ease the coordination of public observation of random selection processes by allowing observers to witness one selection process at the state level, rather than attempt to witness dozens of county-level procedures. Second, the Voter Confidence and Increased Accessibility Act of 2007, mentioned above, would require state-level selection of precincts or machines for an audit.

For audits of close races, the selection of additional precincts over the minimum percentage would work as follows: shortly after the polls close, county election officials would compile the final unofficial election results for all precincts and forward their county-level results to state election officials (as is already done in some states, such as California). State election officials would then determine the unofficial margin of victory in each race and use a confidence-based audit algorithm (discussed below) or table to determine the number of additional precincts that must be audited for each election. State election officials would then randomly select the determined number of additional precincts to audit and notify each county. The county would then audit all of the races in the selected precincts. More detailed suggestions on the selection of additional precincts in close races for audits can be found in Appendix B.

TIERED AUDIT LEVELS BASED ON MARGINS OF VICTORY

Congressman Holt's legislation proposes a variation of the **adjustable-percentage** audit–a "tiered" approach. For all federal races decided by a five percent margin or greater, an audit of three percent of precincts would automatically occur. For federal races decided by less than a two percent margin, the number of precincts audited will increase from three percent to five percent. When a race is decided by less than a one percent margin, ten percent of a Congressional district's precincts will be audited.

We can see how this tiered approach can increase confidence levels by returning to our model Congressional district, introduced in the previous section of this paper on **fixed-percentage** audits. We make the same assumptions as we did before, namely, that there are 400 precincts in the Congressional district of roughly equal size, and a vote shift of more than twenty percent in any precinct would be easily identified, deemed suspicious, and investigated, regardless of any mandated audit.

In this example, we will look at the tiered audit as proposed in Congressman Holt's bill. The highlighted numbers represent the confidence level achieved by the proposal.

TABLE 2. ADJUSTABLE-PERCENTAGE AUDIT MODEL: TIERED AUDITS OF PRECINCTS IN THE MODEL CONGRESSIONAL DISTRICT

No. of Precincts	Margin of Victory	Confidence in a 2% Audit	Confidence in a 3%Audit	Confidence in a 5% Audit	Confidence in a 10% Audit
400	0.75%	15%	22%	34%	**58%**
400	1.75%	31%	43%	**61%**	86%
400	5.00%	66%	**80%**	94%	99%

The numbers in Table 2 were calculated assuming a two-person race, where "margin of victory" is determined by subtracting the total votes for the loser from the total votes for the winner, and dividing by the total number of ballots cast, including undervoted ballots and ballots disqualified in that race. Jurisdictions would have greater confidence that result-changing errors were caught by an **adjustable-percentage** audit than by a **fixed-percentage** audit because the audit level increases as the margin of victory shrinks.

As some commentators have noted, where Congressional districts have fewer than 400 precincts, or where precincts vary substantially in size,[68] these confidence levels will decrease across the board. In practice, determining the number of precincts that must be audited would require a specific calculation that takes into account the distribution (i.e., actual votes per precinct) in the given Congressional district. Nevertheless, the basic concept remains true: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught.[69]

TABLE 3. PREDICTED IMPACT OF A TIERED ADJUSTABLE-PERCENTAGE AUDIT REQUIREMENT ON FEDERAL RACES (2002 – 2006)

Year	Federal Races Requiring a 3% Audit (Margin of Victory Greater than 2%)	Federal Races Requiring a 5% Audit (Margin of Victory Between 1% and 2%)	Federal Races Requiring a 10% Audit (Margin of Victory Between 0% and 1%)
2002	461	3	4
2004	510	5	5
2006	451	7	10

Table 3 shows the predicted impact of a tiered audit in 2002, 2004, and 2006. "Federal races" includes all Congressional races and Presidential races in the fifty states and the District of Columbia. Although a tiered audit adds some complexity to the process, it would probably not add significantly to the cost of conducting the audits – at least if only applied to federal races. The cost of a tiered audit as proposed in Congressman Holt's bill would be negligibly greater than a flat audit of three percent because few races would be subject to a five or ten percent audit. The extra cost of performing some audits in the second and third tier thus contributes about one-thirtieth of the total audit cost.[70] Tiered audits also increase the public's confidence that election results are correctly reported for all races – even close races.

THE CONFIDENCE LEVEL ALGORITHM

To more precisely set the confidence level, some have advocated following a mathematical algorithm that would guarantee a fixed level of confidence (e.g., fifty percent, ninety percent, or ninety-five percent) that a full recount of the paper records would not find error or fraud, if present at a level that would change the outcome of the race being audited.[71]

In implementing such a method, states might require the assistance of statisticians to review the outcome of various races and tell counties how many precincts or machines they need to audit based on the review. To perform this calculation, election officials would need to know not only the unofficial vote totals, but also the number of precincts or machines in which ballots were cast in the race, as well as the variation in the number of ballots cast in those precincts or on those machines.[72] In *Percentage-Based Versus S.A.F.E. Vote Tabulation Auditing: A Graphic Comparison*, several statisticians and political scientists provide an in-depth analysis of how this method could be implemented and detail its various advantages.[73]

A potential advantage of this approach over the tiered audit percentage approach is that jurisdictions will not have to audit more precincts or machines than is necessary to gain confidence that the electronic results have the correct candidate winning. For races that are not close, setting the audit size based on confidence level will likely reduce the audit size significantly from the effort required under a mandatory **fixed-percentage** audit of two or three percent.

2. MODEL STRENGTHS

In addition to the advantage of greater confidence (albeit with greater effort) in close races, the **adjustable-percentage** audit model has many of same strengths as the **fixed-percentage** audit model.

As already discussed, the **adjustable-percentage** audit model has one major advantage over the **fixed-percentage** audit model: it will give jurisdictions and the public greater confidence that there was no error, bug, or attack against the voting system that could change the outcome of a close race, and it will do so more efficiently than requiring a **fixed-percentage** audit of a large number of precincts or machines in *all* races with no regard to the margin of victory between candidates.

3. MODEL WEAKNESSES

We have identified three major weaknesses of the **adjustable-percentage** audit model, one of which is shared with the **fixed-percentage** audit model. As discussed above, audits are effective only if election officials act on the discovery of discrepancies between manual count results and the electronic tally, and even with adjustable-percentage audits, a seemingly innocuous discrepancy of just a few votes between paper and electronic records in one or two precincts could, in fact, indicate far more serious problems.

As recommended in the previous section on the **fixed-percentage** audit model, when discrepancies are found, election officials should conduct additional manual counts of the paper records, investigate the sources of discrepancies, and resolve them. If appropriate, the election officials should order an expanded recount.

Prior to an election, election officials should determine the size of a discrepancy that warrants further recounts or other action. It may not be clear how much of a discrepancy should trigger such actions. An analysis of states with trigger mechanisms could provide guidelines. For example, in Minnesota, the discrepancy rate was one half of one percent, but no counties were actually required to perform additional audits.[74] Although small discrepancies may be unavoidable, ignoring them may result in ignoring outcome-changing problems. While additional experience with audits will help to inform the expectations of election officials, jurisdictions should devise plans for acting on discrepancies.

The second weakness of this model is that election officials face uncertainty about the audit prior to an election. The number of precincts a jurisdiction must audit is based on a mathematical formula that relies in part on the unofficial electronic results totaled after the polls have closed. As a result, election officials may not know how many precincts or machines they will have to audit until Election Day is over. In some high profile state and federal races, election officials could use pre-election polls to assist them in estimating what level of auditing scrutiny might be necessary when the unofficial results are reported. Of course, for many races and issues on a given ballot, there will be little, if any, recent public polling data to assist election officials in making such estimates.

The percent of precincts or machines to be audited could vary from one hundredth of one percent to a full recount. The tiered audit approach attempts to limit this uncertainty by providing acceptable minimum audit sizes (i.e., three, five, or ten percent of precincts).[75] Given how infrequently federal races are decided by small margins, it will be relatively rare that election officials would be required to conduct the "stepped-up" audits in federal elections.

The tiered approach partially addresses this concern by allowing election officials to plan and budget for audits by providing some certainty about audit levels prior to an election. Such certainty does not exist for other variations of the **adjustable-percentage** audit model. The public and losing candidates, however, could feel less confident in the results of very close races. For instance, in our model Congressional district, a ten percent audit of a close race (the maximum audit rate under the Holt proposal) will only have a fifty-eight percent chance of finding an error or fraud that could alter the outcome of a race decided by three-quarters of one percent (and even less of a chance of discovering smaller errors or fraud). In actual Congressional districts with fewer than 400 precincts or where the number of votes cast in precincts varies greatly, the chances of finding such an error would be even smaller.

Finally, if a jurisdiction adopts an **adjustable-percentage** audit model *without a base percentage or number of audits for all races*, it will likely miss some errors or problems with voting machines that a **fixed-percentage** audit might catch when there are no close races. Moreover, without such a minimum audit, election officials are less likely to record, review, and make publicly available information about the votes cast in an election that could assist them in improving the performance of their machines and ballot design in the future. Thus we can imagine a situation where a poor ballot design led a significant number of voters to undervote or cancel their votes upon examining the final DRE review screen, or where a significant number of votes were misread as undervotes because some pens supplied at polling places were not read by the optical scanners. These problems might not be substantial enough to change the outcome of a landslide victory; an audit of just one or a few machines in such landslide races might be all that was necessary to ensure that a winning candidate actually won his race, but such a limited audit is unlikely to reveal the kinds of problems that could presage greater problems if not caught and corrected for future, closer elections.

Accordingly, jurisdictions that implement an **adjustable-percentage** audit model should audit a minimum percentage or number of precincts or machines automatically.

4. ADMINISTRATIVE CONSIDERATIONS

Adjustable-percentage audits are more complex than **fixed-percentage** audits, and because jurisdictions have little experience with the **adjustable-percentage** audits, there are few well-tested procedures. It may be challenging to train staff of an **adjustable-percentage** audit, opening opportunities for human errors.

TIME AND COST OF AUDIT

The cost of conducting an **adjustable-percentage** audit depends heavily on which races are being audited and the margins of victory in those races. Obviously, if there are many close races, a larger percentage of precincts and machines would be audited. On the other hand, this audit method promises to handle audit costs efficiently and fairly. Where races are decided by large margins, it will not be necessary to audit many precincts to obtain a high level of confidence that a full recount would not change the election outcome. Only close races would require a large percentage of precincts or machines to be audited. If a state or the federal government has a role in paying for audits, it would be able to distribute the savings in large-margin (i.e., small audit size) jurisdictions to those with small-margin races that must conduct large audits.

The major administrative burden associated with the **adjustable-percentage** audit model may not be the cost of performing the audits, but the cost of planning for an audit when the number of precincts that might be audited is unknown. The necessity of planning for a large audit might lead jurisdictions to incur expenses for resources (e.g., work space, staffing, etc.) that they ultimately do not use.

The **adjustable-percentage** audit model also may impose unequal financial burdens on election jurisdictions. A jurisdiction that happens to have a race where the two leading candidates are separated by a narrow margin will incur greater expenses than a jurisdiction in which the margin for the same race is relatively wide. Therefore, from a system-wide perspective, it might be necessary to distribute funds on the state or national level to adequately fund jurisdictions that have close races.

OTHER FACTORS

As discussed in the **fixed-percentage** audit model section, the voter-verifiable paper records produced by printer attachments to current DRE voting machine models present unique challenges for jurisdictions that use them. Paper records spoiled by paper jams and printer malfunctions could effectively mask discrepancies. For an **adjustable-percentage** audit, this would lead to an underestimate of the audit size. More generally, spoiled voter-verifiable paper records could drown out the effect of more subtle voting system errors, frustrating the goal of collecting data about voting machine performance during audits.

5. RECOMMENDATIONS TO IMPROVE THE MODEL

We encourage jurisdictions considering this model to adopt the general recommendations (*infra* at page 30) and recommendations to improve the **fixed-percentage** audit model (*supra* at page 17) made in this paper. In addition, we recommend and/or reiterate the following to jurisdictions that adopt an **adjustable-percentage** audit model:

- **Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.** One of the chief benefits of the **adjustable-percentage** audit model is that it allows jurisdictions to reach a relatively high level of confidence that a full recount would not change the outcome of an election in a very efficient manner (i.e., by auditing just enough precincts, machines or other units to ensure that the desired level of confidence is reached). Jurisdictions employing this model might be tempted to audit only one or very few precincts or machines in elections decided by large margins, but doing so would sacrifice several important post-election audit goals related to improving future performance (and, relatedly, the ability to fix problems that could have a greater impact on election outcomes in close races in the future). This includes detecting significant errors that would not change the result of an election, errors that only affect a particular machine model or ballot-type, and errors that might shed light on how voters interact with certain ballot designs. Accordingly, we recommend that jurisdictions employing this method also audit a minimum percentage or number of precincts or machines, including at least one machine model and/or precinct in each county.

- **Account for Precinct Size Variability in Audit Selection and Sample Size Calculations.** Methods to deal with precinct size variability can be as simple as sorting precincts into bins of certain sizes ("small," "medium," and "large"), conducting random selection within each bin or listing precincts in order of size, and ensuring that auditors select a certain number of large precincts. Any analysis, legislation, or administrative procedures that do not take into account the varying number of votes in different precincts are likely to over-estimate the statistical power of uncovering irregularities that could change the outcome of an election.

C. The Polling Audit Model

In contrast to the **fixed-percentage** and **adjustable-percentage** audit models, where all of the paper records for a given number of precincts or machines are manually counted in their entirety, there is another class of post-election auditing proposals that we refer to as instances of a "polling" model.[76]

Under this model, a randomly chosen, small sample of ballots is recounted in *every* precinct and the total of these samples is compared to the unofficial electronic results. We are not aware of any jurisdictions that have adopted this approach, though some election integrity advocates have developed arguments for this audit method.[77]

1. Model Implementation

In practice, election officials would conduct a **polling** audit on election night after the polls close or on the following day. Audit teams would randomly select a small percentage of all paper records in each precinct. The auditors in each precinct would manually count the votes in each race for these sampled records, and a jurisdiction- or state-level official would then total the precinct-level results together. According to the statistical model on which this proposal relies, the hand-counted sample should provide a highly accurate and precise projection of the full electronic tally of the votes (unless that count has been corrupted). The proportion of votes for each candidate in each race of the sampled ballots should very nearly match the proportion of votes for each candidate in the full electronic tally. More specifically, Jonathan D. Simon and Bruce O'Dell, the authors of this proposal, argue that a tally based on a random sample of ten percent of ballots would be within one percent of the full electronic tally ninety-nine percent of the time. In their view, a deviation in the sample count of more than one percent would indicate that the full electronic tally was inaccurate.

The **polling** audit model presents a few logistical considerations that are quite different from the **fixed-percentage** and **adjustable-percentage** audit methods discussed above. First, because a **polling** audit examines individual paper records rather than voting machines or precincts, auditors will likely need to select far more records under this model.

Second, all paper records must have an equal chance of being selected for the recount. Auditors must select the paper records at random, otherwise, the sample of paper records could be biased. For example, selecting the first ten percent of paper records cast could lead to a sample of paper records from voters whose decision to vote early in the day is correlated with certain political preferences. A projection of the full vote tally based on this sample would reflect this bias and accordingly might fall outside the margin of error and call the official results into question. In other words, a failure to draw a random sample of paper records could lead to a falsely positive identification of a significant discrepancy between the paper records and the full electronic tally. As was the case with the **fixed-percentage** and **adjustable-percentage** audit methods, the **polling** audit must include all ballot types. Excluding certain kinds of ballots (e.g., absentee ballots, provisional ballots) would bias the audit sample and leave open several opportunities to attack the official count.

Third, a jurisdiction must develop a means to identify and retrieve the paper records that the auditors randomly select. A conceptually simple method for achieving this end is to mark each paper record with a unique number, and to randomly select paper records from that set of numbers. For paper ballots, such as those read by optical scanners, this process is likely to be straightforward, since the marking process basically amounts to stamping consecutive sheets of paper with sequential numbers.[78] For DREs, which typically use continuous paper rolls for voter-verifiable paper records, the marking and retrieval process could be extremely cumbersome.[79] To mark individual ballot records on these paper rolls would require scrolling through the entire roll, identifying the boundaries of each record, and stamping a number on the record. In any event, this step must occur *after* ballots are cast in order to avoid compromising ballot secrecy.

The second and third requirements are in some tension with a fourth consideration: a **polling** audit should occur as soon as possible following an election. The **polling** audit model is principally intended to address the threat of intentional tampering with centralized ballot-counting equipment in order to produce a desired outcome.[80] To avoid detection, attackers would need to rig the sampling of paper records or corrupt the manual count results of the sampled paper records in order to bring it within the desired margin of error of the full official count. Using publicly verifiable random selection processes and conducting an audit in public mitigate this kind of threat. In addition, authors of the **polling** audit proposal suggest conducting the audits in precincts rather than at a central location.[81] According to the proposal's authors, such a widely distributed audit would require attackers to rely on a larger number of co-conspirators, making it more difficult to maintain the secrecy of an attack and successfully complete it. Finally, the effects of conducting a widely distributed audit on the accuracy of the manual count are unclear; comparing the error rate for this audit design to a centrally conducted audit is an area that may warrant further research.

2. MODEL STRENGTHS

We have identified two major benefits of the **polling** audit model. First, it promises to allow jurisdictions to confirm that the correct candidate has been declared the unofficial winner with a great degree of certainty without requiring jurisdictions to manually count a very large number of ballots. This is true in close races as well.

Second, unlike the **fixed-percentage** and **adjustable-percentage** audit models discussed above, the **polling** audit model would greatly reduce the need to decide whether a discrepancy is large enough to justify additional action. The hand count will or will not produce a result within one percent of the full electronic tally. If it does, Simon and O'Dell argue, we can be ninety-nine percent confident that the electronic tally was correct. On the other hand, if the hand count results are not within one percent of the full electronic results, a full recount or investigation would be necessary. There is little room in this scenario for election official discretion, as there is under the **fixed-percentage** and **adjustable-percentage** audit models.

3. MODEL WEAKNESSES

The **polling audit** model will not necessarily help jurisdictions discover specific errors or fraud. Only when such errors are large and consistent enough to significantly change the number of votes received by each candidate will a **polling** audit alert jurisdictions of such problems.

Similarly, when auditors do find discrepancies, this audit will provide little information about the source of a discrepancy, since the audit is detached from specific precincts and specific machines, and even particular ballot types. This is especially notable for a number of audit goals that use auditing as a feedback mechanism to reform voting systems, procedures, or personnel conduct.

Finally, a consequence of the statistical model underlying the **polling** audit approach is that it will probably produce some "false positives." The model contemplates that, one percent of the time, the hand count of sample paper records and full electronic count will be significantly different, despite the fact that there was no error or fraud. In such cases (in particular, where a false positive indicates that the wrong candidate won in the unofficial results), jurisdictions may be forced to conduct a full recount, only to find that the paper and electronic records match exactly.

4. ADMINISTRATIVE CONSIDERATIONS

TIME AND COST OF AUDIT

It is difficult to compare the costs of **polling** audits to the costs of **fixed-percentage** audits. While **fixed-percentage** audit costs increase roughly in proportion to the audit percentage, it is not clear how costs vary in the **polling** audit model. On one hand, the statistical model underlying the **polling** audit holds that, while the number of ballots that must be sampled varies somewhat with the number of ballots cast in an election (holding other things equal, particularly the confidence level), this variation is minimal.[82] On the other hand, the fact that these audits must be conducted in disparate locations may introduce costs that vary substantially among jurisdictions. Additionally, these audits might be conducted by teams of poll workers fatigued from working at a polling place for several hours. A more realistic staffing scenario would involve hiring additional poll workers or a specialized force of auditors in order to avoid over-burdening polling place staff.

Requiring the audit to occur as soon as possible after an election (see page 27, *supra* for a discussion of why this is particularly important in this audit model) is itself a potential source of administrative burden. Election officials have many responsibilities unrelated to auditing after an election, and audits that require their immediate attention and oversight might distract them from their other duties.

Another ill-defined cost in **polling** audits is that of not knowing where error or fraud may lie. Even if a **polling** audit indicates that there is a discrepancy, it yields little information about what the source might be. Election officials would only know that the hand count result of sampled paper records is out of the agreed-upon error bounds. In contrast to the

fixed-percentage audit model, there is no helpful precinct-level or ballot-type-specific information. **Polling** audits are not useful in deterring attacks on voting systems. In the worst case, the discrepancy would be detected, but not the source. The only recourse election officials have to uncover the source of discrepancies is to conduct a precinct-specific or full **fixed-percentage** audit.

5. RECOMMENDATIONS TO IMPROVE THE MODEL

- **Develop and Test Paper Record Selection Procedures Well Before an Election.** Random selection of paper records is critical to the validity of a **polling** audit. We recommend the ten-sided dice procedure proposed by Cordero, Wagner and Dill, which is easily adapted to this application.[83] Rapid completion of the audit is equally important, as discussed *supra* at page 27. Therefore, a jurisdiction that implements a **polling** audit model should have developed and tested procedures for randomly selecting paper records before the audit occurs – the audit logistics are too complicated, and time is too short, to allow for experimentation after an election.

- **Develop a Plan for Elections Not Confirmed by Polling Audit.** As discussed above, a **polling** audit will provide few clues about whether an unofficial count that differs significantly from the audit count is simply a false positive or whether it is the result of error or fraud. Finding a way to distinguish these two situations might be an area for further research. In addition, if election officials conclude that error or fraud caused the difference, they must have a plan in place to investigate more thoroughly the cause(s). A means for examining ballots and voting equipment to determine whether a certain kind of voting system or ballot type might account for a discrepant result is important.

III. AUDIT BEST PRACTICES

Our review of the audit procedures and other security measures currently in place in most states has led us to conclude that there is a substantial likelihood that such procedures would not detect a cleverly designed software-based attack program. Currently, only fifteen states that require voter-verifiable paper records also mandate regular audits of those paper records.[84] Moreover, even those states that have mandated regular audits have not developed the best practices and protocols that are necessary to ensure their effectiveness in discovering attacks or failures in the voting systems, or in using audits to improve elections in the future. Below we discuss best practices for conducting audits, regardless of what audit model a jurisdiction has chosen, as well as the reasons for instituting such practices:

A. PRACTICES FOR SELECTING VOTES TO BE AUDITED

The method and manner employed by a jurisdiction for choosing votes to audit will have a tremendous impact on whether the audit itself is administratively burdensome, engenders public confidence in election results, detects errors, and provides feedback that will allow jurisdictions to improve elections in the future.

USE TRANSPARENT AND RANDOM SELECTION PROCESSES FOR ALL AUDITING PROCEDURES.

Audits are more likely to prevent fraud and produce greater voter confidence in election results if the public can verify that the paper records, machines or precincts to be audited are chosen in a truly random manner. As noted in *electionline.org*'s March 2007 briefing, *Auditing the Vote,* there is "broad agreement among academics, policymakers, computer scientists and advocates" on this point.[85]

The danger of non-transparent and non-random audits is exemplified by a corrupted recount in Cuyahoga County, Ohio, which took place following accusations of problems in the 2004 general election. The state mandated a hand count of ballots cast in three percent of the county's precincts and a full recount if the three percent audit revealed discrepancies between the punch-card and electronic records. "Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers broke state law by pre-sorting the ballots to ensure they matched the final tally."[86] In other words, the audit was rigged to ensure that no problems were revealed.

To avoid repeating the problems of Cuyahoga County's 2004 audit, the selection of precincts or machines to be audited must be observable by the public and conducted in a truly random manner. In addition, specific guidelines are needed to ensure that observers will be able to actually see each vote counted.

In an ideal transparent and random selection process:

- The whole process is publicly observable and ideally videotaped and archived.
- The random selection is publicly verifiable, i.e., anyone observing is able to verify that the sample was chosen randomly.
- The process is simple and practical within the context of current election practices so as to avoid imposing an unnecessary burden on election officials.[87]

There is today a significant body of literature that addresses ways in which election officials can accomplish these goals. Researchers Arel Cordero, David Wagner and David Dill explained how dice could be used to select precincts randomly in *The Role of Dice in Election Audits*.[88] In the *Machinery of Democracy,* the Brennan Center Task Force on Voting System Security offered its own suggestions for the random selection of precincts or machines to be audited. Both discussions can be found in Appendix C of this paper. These methods are preferable to using a pseudo-random generator on a computer, which is rarely a transparent method for selecting precincts or machines, particularly to observers who do not understand technology. Moreover, as some commentators have noted, because of their opacity, such generators are themselves vulnerable to fraud.[89]

The randomness and transparency of audit selection processes vary in the states that currently conduct audits. In Arizona and Minnesota, precincts and races to be audited are selected by lot (at the county seat in Minnesota).[90] Other states, such as Colorado, New Mexico, Washington, and West Virginia, require jurisdictions to select precincts to audit randomly, but the relevant laws and regulations fail to define "randomness" or describe the selection processes.[91] Parties entitled to appoint poll watchers within the jurisdiction are also entitled to appoint representatives to observe the selection of machines for an audit and the audit itself.[92] In Connecticut, the Secretary of State determines and announces the procedures for randomly selecting DREs to audit, and the selection of machines and the conduct of the audit may be observed by the public.[93] Similarly, in Illinois, the State Board of Elections is charged with designing "a standard and scientific random method" to select five percent of precincts in each jurisdiction to audit "so that every precinct in the election jurisdiction has an equal mathematical chance of being selected."[94] California provides public notice of the time and place of the selection of precincts to be audited and of the audit itself at least five days before either event is scheduled to occur[95] and suggests that election officials use "a random number generator or other methods specified in regulations" to select precincts to audit.[96] In Alaska and Washington, appointed representatives of political parties are permitted to observe an audit, but the opportunity to observe the audit does not extend to members of the general public.[97] Post-election audits in Colorado and in Minnesota are publicly observable.[98]

The time period between the selection of precincts or machines to be audited and the actual audit is security-sensitive. An attacker with the goal of corrupting vote counts could target only those that were not chosen for the audit. Arizona requires jurisdictions to begin post-election audits within the twenty-four hours after the closing of polls.[99] New Mexico conducts a post-election audit within five days of county canvasses.[100] Election officials should minimize this period of time and enforce strict chain-of-custody requirements over election materials used in an audit.

Consider Selecting Precincts or Machines for Auditing at the State Level.

Centralized audit selection is more efficient and transparent. By selecting precincts or machines to audit at the state level, counties are relieved of this responsibility and associated administrative tasks. Additionally, audit selection at the state level facilitates the selection of precincts to audit in election districts that cross jurisdictional boundaries. Finally, public observers of random selection processes would be able to watch a single selection process, rather than attempt to watch multiple county selection processes around a state.

State-level audit selection, however, carries some disadvantages. Some states may be too large – geographically, or in terms of the number of precincts, or both – to select precincts in a reasonable amount of time during a single official event. Selecting precincts or machines to audit in a central location might also make it difficult for local election officials and voters to observe the selection process for their own jurisdiction. This could undermine the transparency that public audit selection should foster. Finally, since audit selections should occur after all ballot types, including absentee and provisional ballots, have been counted, there is a risk that a single jurisdiction with a high proportion of these could hold up statewide selection.

Audit a Minimum Percentage or Number of Precincts or Machines for Each Election, Including At Least One Machine Model and/or Precinct in Each County.

Much of the recent academic literature on post-election audits focuses on catching error or fraud that could change the outcome of an election. But finding an error that has changed the outcome of an election is in many ways a worst case scenario; most would agree that if we are going to find such problems, it would be far better to find (and correct) them in landslide elections where they could have no effect on the outcome of an election. Put another way, in most races, a software bug, attack on vote tallies, or other problem that affected just two percent of the votes would not alter the outcome of an election. Nevertheless most election officials and voters would prefer to find such problems and correct them *before* an audit of an exceptionally close election, rare as they may be. An audit that targets a fixed percentage (e.g., three percent) or minimum number of precincts or machines in each race will assist jurisdictions in detecting widely distributed error or fraud, regardless of whether such error or fraud was substantial enough to change the outcome of the particular election being audited.

Additionally, the inclusion of at least one machine model and/or precinct in each county in an audit should help jurisdictions find discrepancies caused by fraud or error limited to a particular machine or ballot definition file; ballot designs that caused voters to make mistakes; or other problems that might not have been wide-spread enough to change the outcome of a race in the election being audited, but could have such a dramatic affect in future, closer elections.

CONSIDER AUDITING BY MACHINE RATHER THAN BY PRECINCT.

In many states, it will be more efficient to audit by machine or ballot batches, rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same level of confidence in their results by auditing a smaller percentage of machines.

FREEZE AND PUBLISH UNOFFICIAL RESULTS BEFORE SELECTING THE PRECINCTS OR MACHINES TO BE AUDITED.

Election officials should freeze and publish unofficial election results once all returns are received from jurisdictions. The random selection of precincts or machines to be audited should only occur afterwards. Published results should be broken down by precinct or other audit unit (such as voting machine), and further separated into the ballot types that are audited (e.g., if absentees are audited separately from polling place votes, then results should list absentees separately from polling place tallies). If the random drawing is conducted too soon after the close of polls, election workers processing ballots will know in advance which ones will be part of the audit and which will not. For instance, they might be extra-careful when processing ballots from the precincts they know will be audited. Someone intent on committing fraud will be free to do so, knowing that as long as she doesn't touch the ballots that are part of the sample, the audit will have no chance of catching them. Additionally, without the publication of the unofficial results, audit observers cannot verify for themselves that the votes were accurately counted. As a result, election officials supervising the audit may be convinced or assured by its findings, but observers would not necessarily feel similarly confident about the audit.

B. PRACTICES FOR CONDUCTING THE AUDIT

There are specific steps that every jurisdiction can take to make it far more likely that the audit as a whole is accurate, useful to election officials, and likely to catch errors that could change the outcome of specific races.

DON'T JUST MATCH – COUNT!
(RECORD AND PUBLICLY RELEASE MEANINGFUL DATA ON VOTES CAST).

Audits that record and detail the number of overvotes, undervotes, blank votes, spoiled ballots, and, in the case of DREs, cancellations, could be extremely helpful in revealing software attacks and software bugs and in identifying problems in ballot design and ballot instructions.

Most discussions about post-election audits focus on ensuring that the paper and electronic totals of the sampled precincts or machines match. However, a match between paper and electronic records may not reveal the presence of some kinds of problems. These problems may include some types of outcome-changing software bugs, fraud against a voting system, bad ballot design, or machine miscalibration that may have resulted in the disenfranchisement of voters.

Jurisdictions may gain significant information about the performance of their voting machines and ballot design by reviewing and detailing the number of overvotes, undervotes, blank votes, spoiled ballots, and, in the case of DREs, cancellations. This is information that would allow jurisdictions to improve future elections. This type of election data should be tabulated and published, broken down by precinct or machine, and by ballot type (e.g., polling place, absentee, or provisional), if possible. If data on these types of votes deviate from normal values, or are distributed in an uneven manner, a jurisdiction can take action to correct these problems. For example, an anomalously high number of overvotes in a polling place could indicate that it lacks the appropriate feedback to alert voters to how election tabulation equipment is interpreting their ballots. Similarly, an unusually high number of undervotes could point to screen miscalibrations, poor ballot design, poor ballot instructions or other problems.

There are several ways in which such a review would be helpful. First, in the case of DREs, a review of cancellations could show that there were problems with *both* the voter-verifiable paper record and the machine. At least one study has purported to show that the vast majority of voters do not thoroughly check their voter-verifiable paper records.[101] If a voter does not check her paper record, the paper record does not provide extra security for that voter. A vote could be misrecorded on both the paper and electronic record, and both the voter and election officials would not realize votes were incorrectly recorded.

However, if even a small percentage of voters (e.g., twenty percent) check their paper records thoroughly, the identification of an unusual number of cancellations on the paper trail would provide evidence that there was some problem with the mechanism that captures voters' selections on the paper record.[102]

During the 2000 elections in Lake County, Florida, 376 voters' selections for Presidential candidate were disqualified because approximately two-thirds of them displayed a selection of "Gore" from the listed candidates as well as "Gore" in the write-in line.[103] Studies have shown that some voting populations have high rates of overvotes and undervotes on certain types of voting machines. Low-income and minority voters are especially susceptible to this kind of mistake.[104] Now, voters using precinct count optical scan voting machines benefit from those systems' protections against over- and undervotes. If a voter skips a race or selects two candidates in a race, the machine informs the voter of the error and allows her to correct her ballot so that her intention will be accurately recorded.

A software attack that shut off this protection (or a software "bug" that accidentally shut it off) could disproportionately affect certain communities of voters. In *The Machinery of Democracy,* the Brennan Center demonstrated that a state-wide shutdown of this protection could result in the loss of tens of thousands of votes, mostly in low-income and minority communities. A review of the number of over- and undervotes in an audit would provide evidence that something went wrong with this protection and allow election officials to address it.[105]

High overvote and undervote rates may also indicate that ballots were badly designed and caused voter confusion. By recording these data in audits, election officials and the public can gain insight into the effectiveness and usability of various ballot designs.
For precinct count optical scans, auditing of overvote and undervotes can provide election officials with critical information about why some voters' votes aren't recorded. For instance, in Minnesota, a post-election audit report drafted by an election integrity group revealed that the vast majority of discrepancies between hand counts of the paper ballots and the electronic tallies occurred because "the voter used an odd-colored pen, or pressed too lightly with a pencil, in which case the vote was misread as an undervote" or "the ballot got jammed in the optical scanner."[106] Some votes were recorded as undervotes because voters "circled an oval as opposed to filling it in as directed."[107]

Having this kind of information should be extremely useful to election officials. For instance, the Minnesota examples discussed above could help election officials determine: what kind of voter education to focus on to ensure accurate recording of voter intent is maximized; how to improve procedures to ensure that voters are using the right kind of pens; and whether there is some problem with the size or thickness of ballots that might produce an unusually high number of paper jams.

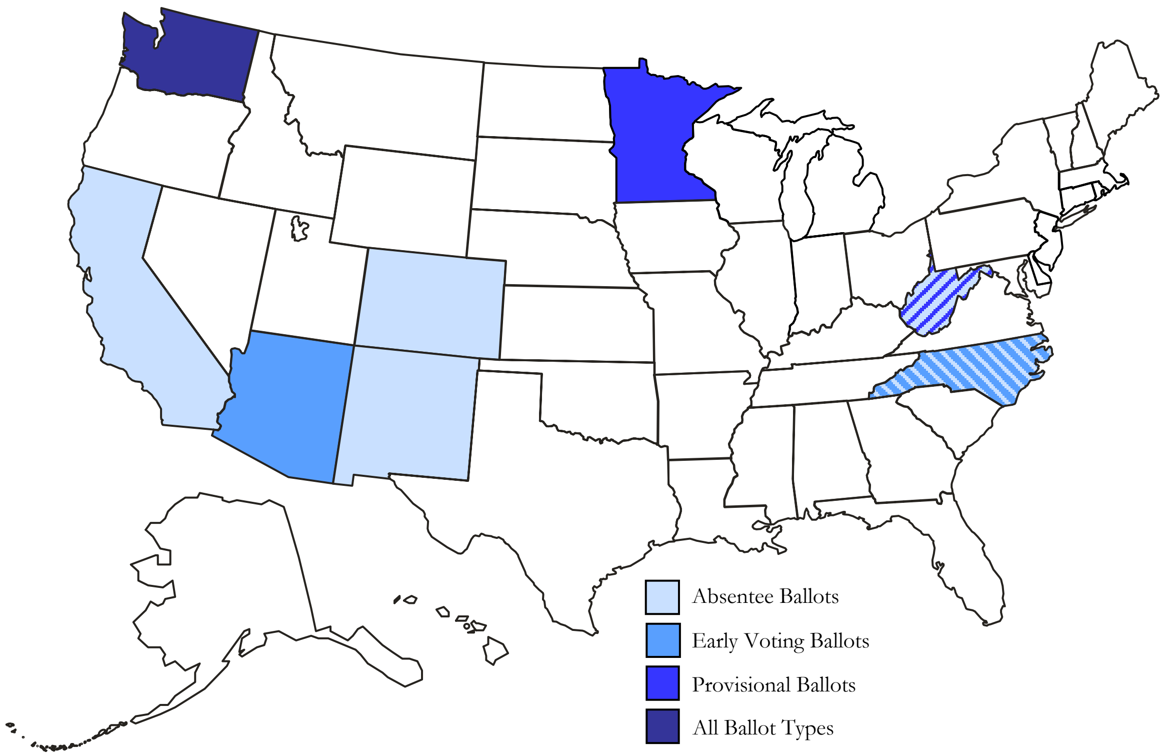
We are aware of only one state – North Carolina – that has collected and made this type of information publicly available, in the hope that it could improve future audits, elections and machines. In reports to the State Board of Election on the May 2006 and November 2006 elections, the University of North Carolina at Chapel Hill's School of Public Health included data that detailed the level of discrepancy between electronic tallies and recounts on each type of machine used, and measured the accuracy of voting machines by reviewing their relative under and overvote counts.[108]

AUDIT ALL METHODS OF VOTING.

In conducting post-election audits, election officials should not exclude any category of votes (e.g., absentee ballots, provisional ballots, damaged ballots). Audits must be comprehensive to ensure that both error and fraud can be readily detected. Although voters cast the majority of ballots on polling place equipment, many jurisdictions increasingly see significant numbers of other ballot types, including early, absentee, provisional and emergency ballots. Fifteen states allow "no-excuse" early voting.[109] In 2004, more than forty percent of all votes cast in Arizona, Nevada, Tennessee, and Texas were received during early voting periods.[110] Voters in twenty-eight states take advantage of "no-excuse" absentee voting by mail. Oregon conducts all elections with mail-in ballots.[111] All but four states have provisional balloting at polling places.[112] The exclusion of any of these ballot types compromises the effectiveness of a post-election audit. To be comprehensive, all ballot types should be included in audit processes. Ballot types should be sorted and stored by precinct, machine, or other unit and randomly selected for auditing.

While the majority of state laws are silent on the inclusion or exclusion of other vote records in a post-election audit, several Western states – where a particularly large number of votes are cast outside the polling place and/or prior to election dates – are not. Specifically, California and New Mexico include absentee ballots cast on electronic voting machines in their audits.[113] In addition to its audit of polling place ballots, Arizona reviews the lesser of one percent of the total number of early ballots, or 5,000 early ballots, randomly selected at the county level from sequestered batches of early ballots from each machine used to tabulate them.[114] Provisional, conditional provisional and write-in votes, however, are excluded from the audit.[115]

FIGURE 3. INCLUSION OF OTHER TYPES OF VOTES IN POST-ELECTION AUDITS



Note: North Carolina includes both absentee ballots and early ballots in an audit. West Virginia audits absentee ballots and provisional ballots.

Source: ARIZ. REV. STAT. ANN. § 16-602(G) (2007); CAL. ELEC. CODE § 15360(a), (b) (West 2007); Colorado Secretary of State Elections Center, *Post-Election Random Audit* at http://www.elections.colorado.gov/DDefault.aspx?tid=833 (last visited July 27, 2007) (absentee precincts included although not clearly statutorily required); Telephone Interview with Brad Anderson, Election Administrator, Minnesota Secretary of State (July 12, 2007); N.M. STAT. ANN. § 1-14-13.1 (West 2007); N.C. GEN. STAT. ANN. § 163.182.2(b)(1a) (West 2007); E-mail from Paul Miller, Elections Information Manager, Elections Division, Washington Secretary of State to Alex Yacoub (July 20, 2007) (on file with the authors); Telephone Interview with Susan Silverman, Special Assistant, Elections Division, West Virginia Secretary of State (July 12, 2007).

C. PRACTICES FOR ENSURING OVERALL AUDIT EFFECTIVENESS

If the audit is to be effective, there are certain basic policies and practices that jurisdictions should have in place. Among the most important are the following:

ENSURE THE PHYSICAL SECURITY OF AUDIT MATERIALS.

Effective auditing of voter-verifiable paper records will serve to deter attacks on voting systems and identify problems only if states have implemented solid procedures to ensure the physical security of election materials used in a post-election audit, such as records of the vote, voting machines, and tally servers. Sound security measures should include a clear chain-of-custody of these materials. Missing or damaged paper or electronic records will make the reconciliation of audits all but impossible.

In *The Machinery of Democracy*, the Brennan Center examined some of the best chain-of-custody practices in jurisdictions across the country. Among the practices cited approvingly in the report were:

- Between elections, voting systems for each county are locked in a single room, in a county warehouse.
- The warehouse has perimeter alarms, secure locks, video surveillance and regular visits by security guards.
- Access to the warehouse is controlled by sign-in procedures, possibly with card keys or similar automatic logging of entry and exit for regular staff.
- Some forms of tamper-evident seals are placed on machines before and after each election. Election officials should place seals over all sensitive areas including vote data media compartments, communication ports and the seams of the voting system case.
- At the close of polls on Election Day, all audit information (i.e., event logs, voter-verifiable paper records, paper ballots, machine printouts of vote totals) that is not electronically transmitted as part of the unofficial upload to the central election office is hand-delivered in official, sealed information packets or boxes. All seals are numbered and tamper-evident.
- The transportation of information packets is completed by two election officials representing opposing parties who have been instructed to remain in joint custody of the information packets or boxes from the moment it leaves the precinct to the moment it arrives at the county election center.
- Once the sealed information packets or boxes have reached the county election center, they are logged. Numbers on the seals are checked to ensure that they have not been replaced. Any broken or replaced seals are logged and the reason for broken or replaced seals is investigated, where necessary. Intact seals are left intact.
- After the packets or boxes have been logged, they are provided with physical security precautions at least as great as those listed for voting machines, above. They should be stored in a room with perimeter alarms, secure locks, video surveillance and

regular visits by security guards and county police officers; and access to the room is controlled by sign-in, possibly with card keys or similar automatic logging of entry and exit for regular staff.

All jurisdictions should detail their chain-of-custody practices for their voting system software, hardware, and audit records (including paper and electronic) in a document that is subject to public review and comment. Public review and comment would increase transparency and accountability for the physical security of audit materials, as members of the public would become invested in the process. The documentation of chain-of-custody requirements allows observers to determine when officials deviate from agreed procedures. Such a document should explain why these procedures are necessary; this would reduce the likelihood of local deviation from the guidelines and ensure that necessary deviations (in the case of an unforeseen incident) held to the spirit of the procedures.

States practices to ensure the physical security of election materials used in an audit vary greatly. In Arizona, election officials at the county level maintain custody of ballots and are responsible for their security during post-election audits.[116] County officials in New Mexico are similarly charged with the secure transport and storage of voting machines after an election.[117] California requires precinct boards to seal and sign containers and packages of ballots and other election materials in the presence of members of the public.[118] At least two members of each precinct board then deliver the sealed containers and packages to election officials at central counting centers.[119] Colorado and Hawaii specify that voted ballots may be handled only in the presence of representatives of different political parties.[120] In Colorado, the receiving election official is required to provide personnel and facilities to preserve and secure election materials.[121] Connecticut requires the collection and storage of voting machines as soon as possible after the completion of an election.[122] Minnesota law requires county auditors to securely store sealed envelopes of voted ballots after an election.[123] In Washington, teams composed of representatives of at least two major political parties pick up sealed containers of voted, untallied ballots from polling places to deliver to the counting center.[124] If ballots are tabulated at the polling place, and if the tallied ballots are sealed in a container, only one elections employee is required to transport them to the elections department.[125]

IMPLEMENT EFFECTIVE PROCEDURES FOR ADDRESSING EVIDENCE OF FRAUD OR ERROR.

If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for addressing audit discrepancies when they are found. Without protocols for responding to discrepancies, the detection of fraud will not prevent attacks from succeeding. Recommended responses include investigating causes of discrepancies, making corrections where necessary, disallowing results if an appropriate remedy cannot be determined, and ensuring accountability for discrepancies (by for instance, banning the voting system in question from further use until the discrepancy has been explained and/or the system is recertified). Jurisdictions should create discrepancy logs that will be made public, and include the results of any investigations undertaken after discrepancies between paper and electronic records were discovered.

AUDIT THE ENTIRE VOTING SYSTEM, NOT JUST THE MACHINES.

Although this study focuses only on post-election audits of voter-verifiable paper records, jurisdictions should conduct audits of the entire voting system to catch errors or fraud in other parts of the voting system. Historically, incorrect vote totals often result from aggregation mistakes at central vote tally locations.[126] Accordingly, good audit protocols will mandate that the entire system – from early and absentee ballots to aggregation at the tally server – be audited for accuracy. Among other procedures, we recommend the following:

- **Ensure That Polling Places Compare Vote Tallies and Sign-in Sheets.** At close of the polls, vote tallies for each machine should be totaled and compared with number of persons that have signed the poll books. A comparison of these numbers should be made publicly available.
- **Ensure Individual Voting Machine and Precinct Totals Are Accurately Reflected in Tally Server Calculations.** A copy of totals for each machine should be posted at each polling place on election night and taken home by poll workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere. This countermeasure allows poll workers and the public to ensure that corrupt or flawed software on a county's central tally server does not incorrectly add up machine vote totals.

Although the adoption of these recommended audit principles may create new financial and administrative considerations for election officials – particularly in states that currently do not conduct any post-election audits – they are necessary costs to ensuring the integrity of election results. The procedures in the few states that currently conduct post-election audits would be substantially improved by the adoption of all of these recommendations.

IV. DIRECTIONS FOR THE FUTURE

The interest of academics and election integrity experts in post-election audits shows no sign of abating. We offer a few suggestions for further study and approaches that, we hope, will add to this research agenda.

A. WORK WITH ELECTION OFFICIALS

Our interviews with election officials have left us convinced that many are eager to use the information developed by academics and election integrity experts to improve their post-election audits. Many ideas discussed in the papers we have reviewed may not be realistic in the context of actual elections, given the financial, logistical and political restraints that election officials face. Ultimately, the best way to develop ideas that can help election officials improve their post-election audits is to work with them, observing the actual conditions under which elections are held.

B. NEW AUDIT METHODS

AUDITING BY BALLOT

The statistics associated with auditing prove that auditors can gain higher confidence in their audit results with a larger audit sample. While this report discusses precinct-level, full recount audit methods as well as machine-level methods, the highest amount of statistical confidence available in our elections would be an audit of individual ballots. If auditors could randomly select a sample of ballots and associate those ballots unequivocally with their corresponding electronic records, auditors would need to examine a smaller amount of ballots in total to reach a similar level of confidence compared to precinct-level or machine-level audits. There are a number of open questions with this style of model. The mapping between paper records and electronic records could compromise ballot secrecy and might be illegal in some states. Also, retrieving individual paper records could be a labor-intensive activity.

HISTORY-DEPENDENT AUDIT MODELS

Some statisticians advocate using historical information to inform audits. For example, in a study of recounts commissioned by the State of North Carolina, Kalsbeek & Zhang recommend calculating a statistic based on historical levels of discrepancy in the chosen precincts.[127] Kalsbeek's method would require a preliminary random selection of at least two precincts per jurisdiction and then a supplementary random selection of a number of additional precincts based on historical data on the level of discrepancies found in previous elections in the precincts chosen in the preliminary selection. These kinds of audit models are interesting, but need more study in order to fully understand what historical data are most useful in modifying audits and how these kinds of audit models can be successfully incorporated into current election regulations and practices.

C. Sharing of Audit Information

We are hopeful that election officials around the country will begin sharing information with each other about how to conduct post-election audits and steps that successfully reduce audit discrepancies. In our interviews with election officials, it was all too often apparent that many were struggling with issues that others had already resolved. Given the importance of this issue, and the fact that there appears to be growing acceptance by jurisdictions across the country that post-election audits are a necessity, we believe it would be particularly helpful if national organizations of election officials such as NASED, NASS and NACO began holding meeting and trainings related to post-election audits, where election officials could share information with academics, election integrity experts, statisticians, auditors and each other. Researchers have also just begun to study procedural issues with conducting manual counts.

D. Future Research

In the course of researching and writing this white paper, we noted a number of topics for future research ripe for exploration. The science of election auditing would be improved immensely by research into counting methods and audit procedures as well as research into the suitability of election technology to support audits.

Manual Counting Methods

There has been very little research to date examining the effectiveness of different methods for recounting votes. The CalTech/MIT Voting Technology Project (VTP) published two working papers on the subject of hand-counted ballots in January 2004 and September 2005, and North Carolina sponsored a statistical analysis of recount discrepancies in May 2006. VTP's first paper examined the frequency with which recounts confirm results in jurisdictions that use optical scan, compared to hand-counted paper ballots in New Hampshire. They found that jurisdictions that used hand-counted paper ballots had a higher rate of tabulation error.[128]

The second VTP paper and the North Carolina study both consisted of statistical analyses of discrepancies between machine and hand counts of ballots.[129] These analyses found small, mostly positive, discrepancies where the magnitude of such discrepancies is larger for hand-marked voting technologies (e.g., punch-card and optical scan ballots) compared to electronic voting machines.

Unfortunately, the specific techniques and procedures associated with the process of manually counting votes have not been studied. There is a widespread belief that humans cannot count as well as computers. However, this criticism depends critically on the procedures used in hand counting and whether or not there is significant variation in how humans and the vote tabulation equipment judge voter intent. Given clear procedures for what constitutes a valid vote and detailed safeguards and checks during the counting process, similar to those used in San Mateo County (see *supra* at page 16), vote counts will be consistently accurate.

There is another technical impetus for further study of hand counting processes: a manual count that matches the electronic tally does not establish the absence of a discrepancy. The error rate of blind manual counts is independent of any discrepancies between the paper records and the electronic tallies. Thus, if there is a one-vote discrepancy between the paper records and the electronic tallies, auditors will face an equal chance of making a mistake that cancels the discrepancy and one that turns it into a two-vote discrepancy. The mistake that cancels out the discrepancy is a false agreement ("false negative") – the recount indicates no discrepancy when, in fact, one exists. One way to guard against false negatives is to conduct additional blind recounts whether there is an apparent discrepancy or not. Additionally, increasing the size of a manual counting team from two people to three or more people would further protect against false negatives. The rate at which these false negatives occur is unknown and likely depends on the manual counting method employed. Quantifying the likelihood of false negatives, and devising other means to address them, are areas for further research.

Election officials need guidance and detailed scientific analyses of manual counting procedures. Members of the NSF ACCURATE center have been working with California counties to document and develop robust manual counting procedures, but this work does not involve controlled experimentation. However, there is a need for an experimental analysis that compares different methods of manual counting procedures for accuracy, efficiency and rates of false negatives.

SUITABILITY OF ELECTION TECHNOLOGY TO SUPPORT AUDITS

Another promising area of research would analyze the effectiveness of currently deployed election technologies. The primary drivers for the design of election technologies cluster around ease-of-use, configurability, speed and durability. Design for voter verification has only been incorporated recently and design for auditability currently meets only a very narrow notion of auditing.

Currently, voter-verifiable paper records produced by electronic voting machines are difficult to handle during a post-election audit. Most, if not all, currently deployed designs for DRE with voter-verifiable paper record printers include a reel-to-reel thermal paper feed for paper records that print using a heat-activated pigment on one side of the paper. Stephen N. Goggin and Michael D. Byrne of Rice University discuss in detail the difficulty of using this printed paper (which is similar to paper used in cash register receipt printers) in post-election audits in a forthcoming article.[130]

Among other problems, these reels of paper records do not protect ballot secrecy; individual records should be cut apart and shuffled. Additionally, because of the reel-to-reel configuration, the individual records curl and don't stack well, which makes handling them during a manual recount cumbersome. Finally, although voting system vendors claim that states can preserve the thermal paper records for the twenty-two month period as required by federal law, it is uncertain whether or not this type of paper is sufficiently durable to withstand a manual recount of multiple races on a single ballot. Research into vote counting methods using thermal paper and research benchmarking the durability of the different kinds of paper that vendors use would reduce election officials' uncertainty as to the types of auditing activities they can undertake.

The software tools provided by vendors play a key role in election auditing. Election databases need to maintain the integrity of the ballots they store and they must also produce reports and output suitable for supporting audits. For example, to do a machine-based audit, auditors would need machine-level results that include aggregate numbers of ballots cast per machine and contest. Each vendors' election database product produces some type of aggregate vote tally output, but not all produce per-machine or per-precinct results separated by each type of ballot (e.g., absentee, early, provisional, regular, etc.). Also, some vendors' products do not provide electronic output in formats that can be provided to citizen's groups for analysis and oversight. Research that catalogs what auditing support each vendor's product provides, what auditors need and what types of capabilities should be standard would eliminate a growing need felt by election officials and potentially eliminate risky ad hoc practices election officials use to cope with current deficiencies.

USING TECHNOLOGY TO AUTOMATE POST-ELECTION AUDITS

A forthcoming paper by Joseph A. Calandrino, J. Alex Halderman and Edward W. Felten of Princeton University looks at how jurisdictions could use recounting machines to conduct most of the work of auditing, reducing the time and money associated with auditing. The authors state that the output of the recounting machines could be "manually audited," and that their proposal would "achieve equal or greater confidence than precinct-based auditing at a significantly lower cost while protecting voter privacy better than previous ballot-based auditing methods.[131] Certainly, the time, labor and financial savings promised by this and similar proposals make the subject of partial automation of post-election audits worthy of further exploration.

GLOSSARY[132]

Acceptance Testing: Acceptance testing refers to the examinations done by a jurisdiction when it purchases equipment from a vendor before delivery is accepted. It is done only once in the history of the equipment, not on a per-election basis. The testing typically consists of a demonstration of basic functionality, such as confirming that the systems boot properly, that they have the proper software versions installed, and that the mechanics (e.g., printers) are in nominal working order.[133]

Cancellation: This term applies only to DRE voting machines that produce a voter-verifiable paper record. If a voter discovers an error on her paper record, she may cancel the erroneous ballot and cast a new ballot. A cancelled or "voided" record refers to the cancelled, erroneous ballot or vote. The cancellation will be documented on the voter-verifiable paper record and may be observed and counted by those conducting audit or recounts of the paper record.

Chain of Custody: The documented order in which election equipment and materials are handled by identified election personnel, including truck drivers and poll workers, as well as officials. Specifically, there should be an unbroken trail of accountability that ensures the physical security of election equipment and materials.

Confidence Level: As referenced in the paper, "confidence level" is the probability (expressed between 0% and 100%) of finding at least one electronically miscounted set of votes (whether they are audited by machine, precinct, or other unit), when there are assumed to be enough such miscounted votes to change the result of the audited election. This is not "confidence level" as used in hypothesis testing for statistical significance. In *Percentage-Based Versus S.A.F.E. Vote Tabulation Auditing: A Graphic Comparison*, written by John McCarthy *et al.*, this concept is referred to as "statistical power," and its mathematical basis and benefits are discussed in detail.[134]

DRE (Direct Recording Electronic Voting Machine): A Direct Recording Electronic (DRE) voting machine directly records the voter's selections in each race or contest. It does so via a ballot that appears on an electronic display screen. Typical DRE machines have flat panel display screens with touch screen input, although other technologies have been used (including paper and push button displays). The defining characteristic of these machines is that votes are captured and stored electronically. Some DREs can be equipped with printers capable of printing voter-verifiable paper records.

Electronic Tally: The electronic count of votes recorded on individual voting machines, possibly aggregated by precinct or polling place.

Logic and Accuracy Testing: Logic and Accuracy Testing is generally conducted prior to the opening of polls and often after the closing as well. It tests the configuration of election definitions on vote tabulation devices to ensure that the content correctly reflects the election being held (i.e., contests, candidates, number to be elected, ballot formats, etc.), that all voting positions can be voted for the maximum number of eligible candidates, and that results are accurately tabulated and reported.

Overvote: An overvote occurs when a voter makes more selections than she is entitled to make. For example, voting for four candidates when the voter is entitled to vote for only three out of seven candidates is an overvote.

Parallel Testing: Parallel Testing, also known as Election Day testing, involves selecting voting machines at random and testing them as realistically as possible during the period that votes are being cast. The fundamental question addressed by such tests arises from the fact that pre-election testing is almost always done using a special test mode in the voting system, and corrupt software could potentially arrange to perform honestly while in test mode while performing dishonestly during a real election. Parallel Testing is particularly valuable to address some of the security questions that have been raised about DREs, but it is potentially applicable to all electronic vote-counting systems.[135]

PCOS (Precinct Count Optical Scan): These machines allow voters to mark paper ballots, typically with pencils or pens. Voters then carry their ballots (sleeved or otherwise protected so that others cannot see their ballot selections) to a scanner. At the scanner, they un-sleeve the ballot and insert it into the scanner, which detects the voters' marks with an optical scanning element and records the votes electronically. The paper ballots are preserved for audits and recounts.

Spoiled Ballot: A spoiled ballot will not count in an election. It is a ballot (optical scan, absentee, or provisional) that a voter returns to election officials to cancel after she has made an error. The concepts of "cancellation" and "spoiled ballot" are often linked, in that statutory limits on the number of ballots a voter may spoil are sometimes interpreted as applying to the number of cancellations a voter can make on a DRE.

Tamper-Evident Seal: Tamper-evident seals are devices used to signal when election equipment or supplies have been improperly handled. They can be as simple as serial-numbered adhesive seals that change color dramatically when disturbed, to serial-numbered strong plastic loop enclosures that cannot be removed without tools. Election equipment and storage containers of ballots and other election materials should be sealed against improper opening. If election equipment or storage containers of election materials have been improperly opened, the seal should show visible signs that such tampering occurred. Jurisdictions should log the removal or disturbance of seals in their chain-of-custody records.

Undervote: An undervote occurs when a voter makes fewer selections than she is entitled to make. For example, voting for only two candidates when the voter is entitled to vote for three out of seven candidates is an undervote.

Voter-Verifiable Paper Record: Voter-verifiable paper records are the paper records or paper trails produced by DRE voting machines that show a voter her selections. She may use the paper record to verify that the machine correctly recorded her selections before casting her ballot. In some states the voter-verifiable paper record is the legal ballot in a recount situation (e.g., California), taking precedence over electronic counts.

APPENDIX A: REPORTED INACCURATE ELECTRONIC VOTE TALLIES AND MACHINE OUTPUT CAUSED BY SOFTWARE BUGS, PROGRAMMING ERRORS, AND OTHER FAILURES*

Compiled by Common Cause and VotersUnite!

* Updated on August 3, 2007.

Date	Machine Type	State	Location/Description
November 2002	ES&S: Optech 3P Eagle	Alabama	**Baldwin County, AL**: An error in the way officials downloaded vote data from a computer cartridge led to an incorrect initial tally of votes in the gubernatorial election. The initial tally of the votes showed that the Democratic incumbent had received 19,070 votes in Baldwin County. A reexamination of the vote tallies showed that the incumbent received only 12,736 votes, which gave the victory to his Republican challenger. The machine in use was an optical scan machine. The incumbent initially called for a recount of all counties and questioned the legitimacy of the election until he finally conceded two weeks later.[1]
November 2006	ES&S: Optech 3P Eagle	Alabama	**Baldwin County, AL**: A voting machine programming error was discovered after the general election. The electronic machine had labeled an unopposed Republican County Commissioner as a Democrat. The error only occurred when voters attempted to cast straight-ticket Republican ballots. Although the election outcome was not affected, since the candidate ran unopposed, the error remained undetected until Election Day had passed, and the candidate received an uncommonly low number of votes.[2]
September 2004	ES&S: Optech IV-C	Arizona	**Maricopa County, AZ**: The original totals in the Republican primary for State House in District 20 showed that one candidate led his closest competitor by only four votes. The small margin led election officials to conduct a recount.[3] The optical scan recount found nearly 500 additional votes for the five candidates in the race, and the initial second place candidate won the election by 13 votes.[4]
November 2004	ES&S: M115	Arkansas	**Carroll County, AR**: An incorrectly programmed chip from an optical scan system skewed results from the race for Justice of the Peace in District 2. Election officials fortunately discovered the glitch when they met to certify the elections. As a result, the ballots were recounted.[5]

Date	Machine Type	State	Location/Description
May 2004	ES&S: M150	Arkansas	**Craighead County, AR**: The initial results of a constable race in District 13 showed that one candidate received all 158 votes cast in Precinct 20. When the opponent questioned the results of the elections, the machine was inspected and an error was found in a computer chip's code. A recount showed that both candidates received votes, though the outcome of the election was unchanged.[6]
May 2004	ES&S: M150	Arkansas	**Fulton County, AR**: A malfunction in a ballot scanner caused county election officials to recount ballots for the primary election by hand. County officials blamed the machine manufacturer for incorrectly programming the machine. The company blamed the county officials for not sending all of the sample ballots needed for the company to program the machines accurately.[7]
November 2006	ES&S: iVotronic	Arkansas	**Cleburne County, AR**: During early voting, some voters reported that the mayoral candidate they selected was switched when they saw their vote on the review screen. The problem was confirmed by the county clerk. The vote-switching was blamed on a calibration error and was not caught until 252 votes had been cast on the questionable voting equipment.[8]
November 2006	ES&S: iVotronic	Arkansas	**Washington County, AR**: The voter-verifiable paper record printed the incorrect voting district numbers for each state representative candidate. A candidate caught the error as he tried to cast his own ballot. ES&S re-programmed the machines and the county election coordinator insisted that the error "never affected the tallying of votes," just the district listed on the audit trail.[9]
August 2004	Sequoia: Edge	California	**Sacramento, CA**: While Sequoia demonstrated their voting machines to the state officials, its touch-screen machine outfitted with a paper trail failed to report votes on Spanish language ballots. "The paper trail itself seemed to work fine but what it revealed was when [the Sequoia representative] demonstrated voting in Spanish, the machine itself did not record his vote," Darren Chesin, staff director for the Senate Elections and Reapportionment Committee, explained. "Programming errors can occur and the paper trail was the way we caught it."[10]

Date	Machine Type	State	Location/Description
March 2004	Diebold: AccuVote-OS	California	**San Diego, CA**: Weeks after election day, local officials discovered an optical scan error. Eight Diebold scanners had been used on 208,446 absentee ballots. Votes were miscounted in both the Democratic presidential primary race and the primary race for the Republican U.S. Senate seat.[11] A recount was conducted, revealing that "2,821 absentee ballots cast for Democratic presidential hopeful John Kerry were actually counted for Dick Gephardt." Similarly, in the Senate race, 68 votes for one candidate and six votes for another were credited to a third candidate. Apparently, the error was caused by multiple scanners feeding data into the tabulation system at once.[12]
November 2005	Diebold: AccuVote-OS	Colorado	**Pitkin County, CO**: Almost 1,200 phantom votes were reported in one precinct. Election officials initially announced that 1,560 people voted in Precinct 5, but later official results showed that 374 people had voted in that precinct. Apparently, the mistake was not caused by an electronic machine error, but instead by faulty spreadsheet formulas used to tally votes from each precinct.[13]
November 2006	Sequoia: Insight 400 C	Colorado	**Denver, CO**: In an election for several local offices, vote counting took nearly a week because 70,000 absentee ballots had been mailed out with barcode misprints. The Sequoia scanners could not sort ballots correctly by district, so election officials had to do so by hand. Additionally, election officials reported that many voters had used incorrect ink pens or marked their ballots in a manner that made it unlikely that the scanners could record their votes. As a result, at least 5% of absentee ballots had to be transcribed onto unused ballots by poll workers in order to be scanned.[14]
November 2002	ES&S: iVotronic	Florida	**Broward County, FL**: A software error caused 103,222 votes, cast with ES&S iVotronic paperless machines, to be left uncounted in the original tally. The error was discovered the morning after Election Day. When the missing votes were added, voter turnout for the county was adjusted from 35% to 45%.[15]

Date	Machine Type	State	Location/Description
November 2004	ES&S: M650	Florida	**Broward County, FL**: A programming error in an optical scan tabulator would have changed the outcome of a ballot measure, had it not been caught by alert election officials. The optical scan tabulator was used to count absentee ballots. The glitch occurred because the machines in use were programmed to accept only 32,000 votes per discrete ballot item, but there were more than twice that number of votes cast on the measure. Once the machines were reprogrammed to allow for counting of all of the votes, the measure received more than 64,000 "yes" votes and it passed. The measure gave the counties permission to seek voter approval for slot machines at several local venues.[16]
October 2006	ES&S: iVotronic; M650	Florida	**Broward County, FL**: During early voting, there were numerous reports of votes cast for the Democratic gubernatorial candidate that were given to his Republican opponent. A spokeswoman for the Supervisor of Elections said that the machines likely needed to be recalibrated and that poll workers were available to fix the machines.[17]
April 2002	ES&S: iVotronic; M650 Unity Election Reporting Management System used to combine totals	Florida	**Miami-Dade County, FL**: In Medley, the vote tallies for two city council races were miscounted when the results of the absentee votes from optical scan machines were combined with the results of the electronic ballots. The initial count showed victories for two candidates who had actually lost the election. The Miami-Dade elections supervisor said that all software had been tested before the election without a hitch, but poll workers noticed the problem as they fed results into the computers. Evidently, a technician from the voting machine manufacturer inadvertently bumped the first candidate to the last position when he opened the ballot program on the memory cards to change the heading of the ballot. When the results of the two systems were combined, they didn't match properly.[18]
November 2006	Sequoia: AVC Edge	Florida	**Palm Beach County, FL**: Voters reported that vote-switching had occurred as they cast their ballots in the 2006 House race. Additionally, others experienced problems when the wrong ballots appeared on their touch screens while voting.[19]

Date	Machine Type	State	Location/Description
November 2006	ES&S: iVotronic	Florida	**Sarasota County, FL**: There were over 18,000 undervotes in the 13th Congressional race between Vern Buchanan (R) and Christine Jennings (D).[20] Buchanan defeated Democrat Christine Jennings by a slim 369 vote margin.[21] There were numerous complaints that the 13th Congressional District race was not appearing or recording properly. Some voters reported that votes for Christine Jennings failed to appear on the review screens at several polling locations.[22]
September 2002	ES&S: M100	Florida	**Union County, FL**: In Union County, Florida, a programming error caused machines to read 2,642 Democratic and Republican votes as entirely Republican in the September 2002 election. The vendor, ES&S, accepted responsibility for the programming error and paid for a hand recount.[23]
November 2006	Diebold: TS-R6; TS-RS	Georgia	**DeKalb, Fulton, and Cobb Counties, GA**: Touch-screen voting machines switched votes for Democratic candidates to Republicans. Technicians were dispatched to recalibrate machines. The vote-switching problems significantly slowed down the voting process for those who went to the polls. By mid afternoon, at least 30-40 voters reported experiencing the vote-switching problem.[24]
September 2004	Hart: eSlate 3000	Hawaii	**Honolulu, HI**: Voting machines gave voters the option of selecting a Green Party ballot, although there were no Green Party candidates. As a result, 22 voters wasted their votes and were essentially disenfranchised.[25]
November 2006	ES&S: M550	Idaho	**Bannock County, ID**: Although county election officials were directed by ES&S to use Bic pens to mark ballots, the scanners failed to recognize the ink. Once the uncounted ballots were identified, poll workers marked each ballot with ink that would be recognized by the scanner and fed them into the machine for a second time.[26]
October 2006	Sequoia: AVC Edge II Pl	Illinois	**Chicago and Cook County, IL**: Trouble reports filed by voters and poll workers during early voting detailed some calibration issues with the touch screens. According to the Chicago Tribune, Chicago and Cook County officials said they had received a few complaints from early voters about pressing once candidate name on the touch screen and having the machine register another. This type of event can occur if the machine is not adequately calibrated.[27]

Date	Machine Type	State	Location/Description
April 2003	ES&S: M100	Illinois	**Lake County, IL**: Because of a programming error that failed to account for the option of "no candidate" on the ballot, election results were placed next to the names of the wrong candidates in four different races. The problem was corrected by 10pm on the evening of Election Day.[28]
November 2004	Fidlar: AccuVote 2000 ES	Indiana	**Franklin County, IN**: A glitch caused optical scanners to count Democratic straight-line votes as Libertarian votes. After the error was found, the recount changed the results of the county commissioner's race in favor of the Democratic candidate. The glitch was suspected when a Libertarian congressional candidate was receiving four times the vote in Franklin County than in the rest of the district. The voting machine manufacturers called the glitch an "isolated incident."[29]
November 2004	ES&S: Microvote Infinity	Indiana	**LaPorte County, IN**: Electronic voting machines reported that each precinct had exactly 300 registered voters. Election officials did not notice the error until 7:00pm on election night. If there had actually been 300 voters in each precinct, there would have been 22,200 in LaPorte County as a whole. In fact, there were more than 79,000 registered voters in the county.[30] Reports were unclear as to whether votes were lost as a result.
November 2006	ES&S: iVotronic	Indiana	**Marion County, IN**: When the polls closed at 6:00pm on Election Day, workers were unable to retrieve votes from the 520 touch-screen machines used by disabled voters. The problem occurred because ES&S had programmed the machines for Pennsylvania's polling hours, which stayed open until 8:00pm. Disabled voters were concerned that their votes would not be counted. In fact, when the incident was reported three days after the election, those same votes had not yet been recovered or counted.[31]
June 2006	ES&S: M100	Iowa	**Pottawattamie County, IA**: A ballot programming error caused the new optical scan system to tabulate votes incorrectly. When absentee ballots were tabulated for a county recorder's race in the Republican primary, results showed one candidate, a University of Nebraska at Omaha student, had 99 votes, while his opponent, the county recorder since 1983, had only 79. The surprising outcome led to a recount of absentee ballots, revealing that the incumbent actually received 153 votes while his challenger received 25.[32]

Date	Machine Type	State	Location/Description
November 2004	ES&S: Optech III	Iowa	**Scott County, IA**: Optical scan machines malfunctioned when tabulating absentee ballots. As a result, poll workers had to manually feed about 23,000 ballots one by one.[33]
August 2002	ES&S: Optical Scan (model unknown)	Kansas	**Clay County, KS**: A computer glitch in an optical scan voting system showed that a challenger in a primary race for county commissioner had won, but a hand recount showed that the incumbent commissioner won by a landslide: 540 votes to 175. The computer had mistakenly reversed the totals for the candidates in one ward.[34]
November 2006	Hart: eSlate	Kentucky	**Calloway County, KY**: Vote-switching appeared to have occurred on the review screens of Hart InterCivic eSlate machines. Straight-ticket Democratic votes were switched to Republican straight-ticket votes in all contested races.[35]
November 2006	ES&S: 3P Eagle	Maine	**Waterville, ME**: Unidentified machine malfunctions caused election results to indicate that one Senate candidate for District 25 received 27,000 votes on one of the three machines used by the town. 27,000 is about 16,000 more votes than the number of registered voters in the whole city.[36]
May 2006	Diebold: AV-OS	Michigan	**Barry County, MI**: Flawed ballot programming caused an optical scan system to tally votes incorrectly. The problem was discovered when a county clerk received the voting results from the precinct where he had voted and saw that one candidate received no votes, despite the fact that he voted for the candidate himself. He also thought it peculiar that 90 out of 127 votes cast in one precinct selected the option to write in a candidate on the ballot. Because there were widespread problems with machines incorrectly tallying votes, county workers hand counted votes for the school board election.[37]
August 2004	Sequoia: Optech III-P Eagle	Michigan	**Muskegon, MI**: In the race for Township Clerk, Optech scan machines failed to detect 2% of votes. Initially, the machines indicated that the incumbent had been defeated by a five vote margin. After a recount, 39 additional votes were factored into election totals and the challenger won by two votes.[38]

Date	Machine Type	State	Location/Description
May 2005	ES&S: Optical Scan (model unknown)	Mississippi	**Forrest County, MS**: The primary election for a city council race was not certified for days after the election because of discrepancies in vote tallies. The number of ballots counted by optical scanners reportedly did not correspond to the vote totals on the voting machines.[39]
May 2006	ES&S: M150, M550	Montana	**Yellowstone County, MT**: A programming error caused voting machines to inaccurately record all votes. An election official explained that he suspected the problem had occurred because he forgot to hit the "zero out" button required between entering absentee and regular ballots on the machine. Consequently, as many as 3,000 absentee ballots may have been counted a second time when the regular ballots were being run through the machines. Officials decided to conduct a full recount to ensure that the election outcome was accurate.[40]
November 2004	ES&S: M550	Nebraska	**Lancaster County, NE**: During the general election optical scan machines experienced a number of malfunctions. Some shut down completely. When the problems began, election officials stopped to test the six machines, revealing that two were not producing correct vote tallies. Those two machines were shut down, but later in the day, the remaining machines began to have similar mechanical problems.[41]
November 2002	ES&S: M100	Nebraska	**Sarpy County, NE**: The optical scan machines failed to tally "yes" votes on the Gretna school-bond issue, giving the false impression that the measure was defeated. The measure had actually passed by a 2-1 margin.[42]
November 2004	ES&S: M650	Nebraska	**Sarpy County, NE**: After ballots were counted in a race for city council, election officials realized that there were more votes than voters. According to the officials, the error affected 32 of 80 precincts and as many as 10,000 votes. It was believed that the glitch affected the candidates equally and did not alter the outcome of the elections. The evidence and explanation for the miscount were inconclusive.[43]

Date	Machine Type	State	Location/Description
November 2006	Sequoia: AVC Advantage	New Jersey	**Passaic, Paterson, Scotch Plains, and North Bergen Counties, NJ**: The US Attorney for New Jersey dispatched investigators to address complaints of voting machines that were preventing voters from casting ballots for the Republican Senate candidate. Some reported that their ballot was pre-voted in favor of the Democratic incumbent, while others said the machine would not register their selections.[44]
November 2002	Sequoia: Edge	New Mexico	**Bernalillo County, NM**: After Election Day, local officials discovered that about 12,000 early votes remained uncounted. Reportedly, the error was confined to early voting machines, on which approximately 48,000 people cast their ballots. Apparently, vote total changes did not alter the outcome of the race.[45]
November 2004	Sequoia: Edge; AVC Advantage ES&S: iVotronic Danaher: Shouptronic	New Mexico	**Bernalillo County and other counties, NM**: Throughout the state of New Mexico, significantly high phantom vote rates and undervote rates led voting analysts to question the outcome of the elections in New Mexico. New Mexico led the nation in the highest undervote rates. Also, certified results showed a remarkably high number of phantom votes.[46]
November 2004	Sequoia: AVC Advantage	North Carolina	**Buncombe County, NC**: Touch-screen voting machines in at least two precincts did not display one of the races on the ballot. One election official estimated that the error affected at least 600 voters. Because there was no paper record, it was impossible to determine how many votes were lost.[47]
November 2004	Unilect: Patriot	North Carolina	**Carteret County, NC**: In the election for state agricultural commissioner, about 4,400 votes were lost. On election night, 3.3 million ballots were cast and the Republican candidate led his Democratic opponent by 2,287 votes. The touch-screen DREs that had caused the problems did not have a backup system, making the lost votes irrecoverable. With almost twice as many votes permanently erased as were needed to win the election, a contentious legal battle ensued that only ended three months later when the contesting candidate decided to concede the election.[48]
November 2002	ES&S: Optech 3P	North Carolina	**Chatham County, NC**: A machine programming error caused all straight-ticket Republican votes to go to the Libertarian candidate in N.C. House District 54.[49]

Date	Machine Type	State	Location/Description
September 2002	ES&S: M100	North Carolina	**Robeson County, NC**: During a Senate primary, ballot-tabulating machines malfunctioned in 31 of 41 precincts. Local election officials stated that it was due to a software glitch related to faulty memory card programming and recounted the ballots.[50]
November 2002	ES&S: Optech 3P Eagle	North Carolina	**Wayne County, NC**: A programming error caused machines to skip several thousand party-line votes, both Republican and Democrat. Correcting the error turned up 5,500 more votes and reversed the outcome of the race for State House District 11.[51]
November 2004?	ES&S: iVotronic	Ohio	**Mahoning County, OH**: Sixteen of the 312 precincts experienced problems with voting machines on Election Day, resulting in delays when tabulating the results. The problems were attributed to a number of issues, including machine malfunctions, problems with cartridges, and human error.[52]
November 2004	ES&S: M550	Ohio	**Sandusky County, OH**: An election turnout of 131% in one town indicated a tabulation error. Officials concluded that some ballots, in nine precincts, had been counted twice. They speculated that some ballots had been fed through the machine more than once.[53]
November 2006	ES&S: iVotronic	Pennsylvania	**Allegheny County, PA**: Twenty voting machines were removed from polling stations across Allegheny County due to technical glitches. The faulty machines failed to "zero out," or reset the vote tally at zero before the voting started.[54]
July 2005	Danaher: 1242	Pennsylvania	**Berks County, PA**: During the primaries for county election board, 111 votes were lost. The error occurred when the cartridges used to record votes were accidentally programmed as training cartridges. Election results showed that three races were determined by less than 111 votes.[55]
May 2005	ES&S: M550	Pennsylvania	**Cumberland County, PA**: A ballot programming error for straight-line ticket votes gave the office of magisterial district judge to the wrong candidate. Straight-ticket Democratic votes were given to the Republican candidate. Straight-ticket Republican votes were not counted at all. Initial vote totals showed the Republican candidate had won by a 1,650 to 1,468 margin. Ultimately, however, the Democratic candidate won by a two-vote margin – 1,703 to 1,701 – in the recount.[56]

Date	Machine Type	State	Location/Description
May 2006	ES&S: Optical Scan (model unknown)	Pennsylvania	**Luzerne County, PA**: Unofficial tallies differed by nearly 6,000 votes from official ballot counts. Some candidates' vote totals were hundreds of votes short of the initial count. The tabulation errors were attributed to the voting machine vender, who failed to reset a counter on a ballot scanner.[57]
November 2006	ES&S: iVotronic	South Carolina	**Charleston County, SC**: iVotronic machines failed to allow voters to review their choices in contests in which they voted for more than one candidate. "If voters can vote for only one candidate, the review screen shows who they voted for, but if they can vote for two or more candidates, as is the case in a Charleston County School Board race and the Charleston County Soil and Water Commission race, then the review screen indicates only whether they have voted for the maximum number allowed. It does not state for whom they voted."[58]
November 2005	ES&S: iVotronic	South Carolina	**Kershaw County, SC**: Initial vote totals in the Republican and Democratic primary races for a County Council seat, showed that 3,208 votes had been cast in District 2. A manual count discovered that only 768 votes had been cast. Election officials suspected that the error had occurred because machine cartridges were incorrectly programmed to record some votes more than once. A state election official apparently did not check a box that would have prevented multiple readings.[59]
October 2006	ES&S: iVotronic; M650	Texas	**Bexar County, TX**: The tabulation of election results was delayed for one and a half hours. The tabulation computers had not been programmed with updated data in order to count "mail-in" paper ballots. The computer system was taken off-line and updated with the information needed to process the 3,000 paper ballots, which were then tabulated using high-speed scanners.[60]
November 2006	Diebold: TS-R6	Texas	**El Paso County, TX**: El Paso County Attorney Jose Rodriguez said that 16 people complained that a vote cast on their touch-screen ballot registered to the wrong candidate. Five of the people called Rodriguez' office to complain. Eleven others called a local radio show to complain.[61]

Date	Machine Type	State	Location/Description
November 2006	ES&S: iVotronic	Texas	**Hidalgo County, TX**: Election officials had to recount votes for U.S. House District 28 manually after discovering that the device used to download election totals from its touch-screen machine malfunctioned. "The director of elections for the Texas Secretary of State's office, Ann McGeehan, said votes would be counted using a printout generated by each voting machine."[62]
October 2006	ES&S: iVotronic	Texas	**Jefferson County, TX**: During early voting, voters complained that when they selected a particular candidate, another candidate's name would light up. KDFM reported that the vote switching occurred with voters who had cast a straight Democratic ticket as well as individual votes.[63]
March 2004	ES&S: M315	Texas	**Lubbock County, TX**: Machines failed to count votes in the race for Precinct 8 Democratic chairman. The ballots had to be recounted with alternate software, provided by ES&S.[64]
November 2002	ES&S: M650	Texas	**Scurry County, TX**: An unanticipated landslide victory for two Republican commissioner candidates caused poll workers to question the results. A chip in the ES&S M-650 contained an incorrect ballot program. After ES&S sent a new chip and the county officials counted the votes by hand, the opposing Democratic candidates actually won by a large margin.[65]
March 2006	Hart: eSlate; eScan	Texas	**Tarrant County, TX**: During the primaries in Tarrant County, TX, a programming error caused an extra 100,000 votes to be recorded than had been cast. Initial tallies indicated that 158,000 people had voted when actually only approximately 58,000 had voted. The problems stemmed from a programming error created by the vendor, Hart InterCivic. The error caused the computer to compound vote totals each time the election totals were updated throughout the night, rather than simply keeping a running total. According to news accounts, John Covell, a vice president with Hart stated, "The system did what we told it to do. We told it incorrectly." The program was designed specifically for Tarrant County, and no other counties reported similar problems, elections officials said.[66]

Date	Machine Type	State	Location/Description
October 2004	Hart: eSlate	Texas	**Travis County, TX**: Voters complained that their votes had been changed for the Presidential race. Voters who cast a straight-party Democratic ticket reported that after a final review of their ballot that the presidential selection had been shifted from Kerry/Edwards to Bush/Cheney. Travis County election officials tested the voting system and could not replicate the errors. Gail Fisher, manager of the county's Elections Division, theorized that after selecting their straight party vote, some voters went to the next page of the electronic ballot and pressed "enter" perhaps thinking they were pressing "cast ballot" or "next page." Since the Bush/Cheney ticket was the first item on the next page, the voters were accidentally reselecting a new presidential team.[67]
November 2003	AVS: WinVote	Virginia	**Fairfax County, VA**: Voters complained that the machines were failing to register their votes for incumbent school board member Rita S. Thompson (R). Local election officials reported that testing later indicated that for every 100 votes cast for Thompson, the machines subtracted approximately one vote for her. According to voters, the machine would initially display an "x" aside Thompson's name, but the "x" would disappear seconds later. One voter said it took him about 4 or 5 attempts before he successfully voted for Thompson. It was impossible to determine whether lost votes were intended for Thompson or whether other candidates also lost votes.[68]
November 2006	AVS: WinVote	Virginia	**Fairfax, VA**: Reports indicated that if voters touched the screen around the U.S. Senate box, the wrong candidate would light up. Election officers told voters to make sure to use their fingertips and to notify them of any malfunctions they encountered. Fairfax's general registrar called the WinVote manufacturer to report the glitch and was told it was a calibration issue and couldn't be immediately fixed.[69]

Date	Machine Type	State	Location/Description
November 2004	Sequoia: AVC Edge	Washington	**Snohomish County, WA**: Voters in at least four polling precincts reported that they experienced vote-switching errors. They explained that the review screen showed they had chosen the opposing candidate. It took several attempts for each voter to correct the mistakes. Review screens showed that the correct candidates had been selected. Snohomish County elections official Bob Terwilliger reported that the problem only occurred in 15 out of 950 electronic voting machines throughout the county.[70]
November 2006	ES&S: M150	Wisconsin	**Taylor County, WI**: Four and a half months after the election, a consulting firm discovered that the optical scanners were programmed incorrectly. All straight-party votes were lost, affecting approximately 600 ballots.[71]
November 2004	ES&S: Optech III-P Eagle	Wyoming	**Natrona County, WY**: In several municipal races, the Unity Election Management System, used to tally votes from both optical scan machines and paperless electronic voting machines, failed to tally votes correctly. Noticing that the ballot totals in the city of Evansville seemed low, election officials checked the printouts from the precinct voting machines. They found that the totals didn't match the totals computed by the Unity software. Election officials conducted a recount using printouts from the voting machines and the paper absentee ballots.[72]

ACKNOWLEDGMENTS

This chart on voting machine tally failures was produced by staff at Common Cause but could not have been created without the hard work and dedication of a number of people. Ellen Theisen and John Gideon of VotersUnite! provided extensive documentation of voting machine errors and also provided a comprehensive compilation of news stories related to voting machine problems which served as a template for this chart. Several individuals at Common Cause were also indispensable. Liz Dries spent countless hours researching the data and tracking down news articles. Thanks also go to Susannah Goodman, Matt Shaffer, Erin Huckle and Cinthya Guevara for research, editing and fact checking. Special thanks to Pam Smith and Warren Stewart of Verified Voting Foundation who shared their extensive knowledge of voting system venders with our team.

NOTES

[1] John Archibald & Brett J. Blackenridge, *Early Printout Was Only Source of Wrong Tally*, BIRMINGHAM NEWS (Nov. 10, 2002); Jeffrey Gettleman, *Alabama Governor Ends Challenge of Vote Count*, NEW YORK TIMES (Nov. 19, 2002).
[2] *Another Voting Glitch in Baldwin County*, ASSOCIATED PRESS (Nov. 14, 2006).
[3] *McComish GOP Winner in District 20 by 13 Votes, Recount Shows*, THE ARIZONA REPUBLIC (Sept. 21, 2004).
[4] Nedra Lindsey, *McComish's District 20 2nd-place Finish Confirmed*, THE ARIZONA REPUBLIC (Sept. 24, 2004).

[5] Anna Mathews, *Computer Glitch Blamed for Miscount in JP Voting*, CARROLL COUNTY STAR TRIBUNE (Nov. 10, 2004).
[6] LeAnn Askins, *Commission OKs Results of Elections*, JONESBORO SUN (May 28, 2004).
[7] George Jared, *No Explanation for Ballot Machine Malfunction*, SOUTH MISSOURIAN (May 27, 2004).
[8] Louis Short, *Vote Machine Problems Reported*, (Heber Springs, AR) SUN-TIMES (Nov. 27, 2006).
[9] Trish Hollenbeck, *Voting Machines To Get Fix After Audit Trail Prints Right Vote For The Wrong District*, NORTHWEST ARKANSAS TIMES (Oct. 26, 2006).
[10] Ian Hoffman, *Lawmakers Cut E-Voting's Paper Trail: Manufacturers Demonstrating New Printers In Nevada Were Embarrassed When Machine Failed To Recognize Votes*, TRI-VALLEY HERALD (Aug. 13, 2004); Kim Zetter, *Wrong Time for an E-Vote Glitch*, WIRED NEWS (Aug. 12, 2004).
[11] Conaughton Gig, *New Electronic Scanners Miscounted Some County Votes*, NORTH COUNTY TIMES (Apr. 7, 2004).
[12] Luis Monteagudo Jr. & Helen Gao, *Some Votes Miscounted In Primary, Officials Say*, UNION-TRIBUNE (Apr. 8, 2004).
[13] Allyn Harvey, *Phantom Votes Haunt Pitkin County Election Officials*, ASPEN TIMES (Nov. 3, 2005).
[14] Ann Imse, *Big Bar Code Backfire*, ROCKY MOUNTAIN NEWS (Nov. 14, 2006).
[15] *Election Glitch Missed 103,000 Votes in Florida County*, CNN (Nov. 8, 2002).
[16] Jeremy Milarsky & Rafael A. Olmeda, *Broward County, Fla., Fixes Computer Error To Correct Statewide Gambling Vote*, SOUTH FLORIDA SUN-SENTINEL (Nov. 5, 2004).
[17] Charles Rabin & Darran Simon, *Glitches Cited in Early Voting; Early Voters Are Urged To Cast Their Ballots With Care Following Scattered Reports Of Problems With Heavily Used Machines*, THE MIAMI HERALD (Oct. 28, 2006).
[18] Oscar Corral, *Technician's Error, Not Machines, To Blame In Dade Election Mix-Up*, THE MIAMI HERALD (Apr. 4, 2002).
[19] Luis F. Perez, *Palm Beach County Records 32,000 Early Votes for Tuesday's Election*, SOUTH FLORIDA SUN-SENTINEL (Nov. 2, 2006).
[20] *Dozens of Voters Complain about Glitch*, HERALD TRIBUNE (Nov. 8, 2006).
[21] Doug Sword & Anna Scott, *House Could End up in 13th District Dispute*, SARASOTA HERALD-TRIBUNE (Nov. 9, 2006).
[22] Todd Ruger, *Voting Glitch Prompts Warning*, SARASOTA HERALD TRIBUNE. (Nov. 5, 2006).
[23] Bev Harris, *Can We Trust These Machines?*, BLACK BOX VOTING 4 *available at* http://www.blackboxvoting.org/bbv_chapter-2.pdf.
[24] Rhonda Cook, *Georgia Votes 2006: Machine Glitches: Smooth Day? No Way*, ATLANTA JOURNAL-CONSTITUTION (Nov. 8, 2006).
[25] *Primary Election Runs Into Problems; Some Problems Caused by Electronic System*, KITV 4 NEWS (Sept. 24, 2004).
[26] Rebecca Boone, *Dems Critical of Idaho Election Officials*, CASPER STAR TRIBUNE (Nov. 9, 2006).
[27] John McCormick, *Voting Equipment Glitches Lingering*, CHICAGO TRIBUNE (Nov. 2, 2006).
[28] Susan Kuczka, *Returns Are In: Software Goofed – Lake County Tally Misled 15 Hopefuls*, CHICAGO TRIBUNE (Apr. 4, 2003).
[29] *Computer Error On Ballot Count Changes Results For County Commissioner In Indiana*, ASSOCIATED PRESS (Nov. 12, 2004).
[30] William Rivers Pitt, *Worse Than 2000: Tuesday's Electoral Disaste*, Truthout.org (Nov. 8, 2004), *available at* http://www.truthout.org/docs_04/110804A.shtml.
[31] *Disabled Voters Disappointed with Touch-Screen Problems*, WISH-TV (Nov. 10, 2006).
[32] Tim Rohwer, *Faulty Voting Machines Delay Results; Counting Under Way*, THE DAILY NONPAREIL ONLINE (June 7, 2006).
[33] Lynn Campbell, *Broken Vote-Counting Machines, Moveon Draw Complaints In Iowa*, DES MOINES REGISTER (Nov. 3, 2004).
[34] *Aug. 6 Ballot Problems Alleged; Clay, Barton County Candidates Seek Review Of Races*, LAWRENCE JOURNAL-WORLD & NEWS (Aug. 22, 2002).
[35] Warren Stewart, *All Four Major E-Voting Machines Flip Votes in Early Voting*, VoteTrustUSA (Nov. 5, 2006), *available at* http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1967&Itemid=26.
[36] Colin Hickey, *Results Slowed by Machine Trouble*, JOURNAL & MORNING SENTINEL (Nov. 9, 2006).
[37] Ben Cunningham, *Malfunction Delays Hasting Results*, GRAND RAPIDS PRESS (May 4, 2006).
[38] Steve Gunn & Lynn Moore, *Election Turns Around When Inspectors 'See The Light'*, MUSKEGON CHRONICLE (Sept. 4, 2004).
[39] *Problems Delay Final Vote Count*, HATTIESBURG-AMERICAN (May 7, 2005).

[40] Ed Kemmick, *Software Flub Leads to County Recount*, BILLINGS GAZETTE (Nov. 8, 2006).
[41] Nate Jennings, *Problem Machines Spur Call for Recount*, LINCOLN JOURNAL STAR (Nov. 14, 2004).
[42] Joe Dejka & Chris Olson, *A late Night in Sarpy; Glitches Delay Results*, OMAHA WORLD-HERALD (Nov. 6, 2002).
[43] *Countinghouse Blues: Too Many Votes*, WOWT 6 OMAHA (Nov. 5, 2004).
[44] Dave Evans, *Voting Problems Reported in NJ*, WABC-TV NEW JERSEY (Nov. 7, 2006).
[45] *12,000 Early Votes Skipped in Count*, ALBUQUERQUE TRIBUNE (Nov. 16, 2002).
[46] Warren Stewart & Ellen Theisen, *Summary Report on New Mexico State Election Data* (www.HelpAmericaRecount.org Jan. 4, 2005), *available at* http://www.democracyfornewmexico.com/democracy_for_new_mexico/files/NewMexico2004ElectionDataReport-v2.pdf.
[47] Cecil Bothwell, *Buncombe Machines Disenfranchise Voters*, MOUNTAIN XPRESS (Nov. 10, 2004).
[48] Gary D. Robertson, *Months After Election, North Carolina's Agriculture Commissioner Agrees He Lost*, ASSOCIATED PRESS (Feb. 5, 2005).
[49] Jessica Rocha, *Mechanic to Smooth Vote*, NEWS & OBSERVER (Oct. 14, 2004).
[50] Ellen Theisen, *Ballot Definition Files: No Review Is Provided for a Key Component of Voting System Software*, VotersUnite! (June 2004, updated Oct. 2005 & June 2006), *available at* http://www.votersunite.org/info/BallotProgramming.pdf.
[51] Wade Rawlins & Rob Christensen, *"Winners" May Be Losers*, NEWS & OBSERVER (Nov. 12, 2002).
[52] *Errors Plague Voting Process in Ohio, Pa*, VINDICATOR (Nov. 3, 2004); Brian Gottstein, *Back up! We Need Back Up!*, ROANOKE TIMES (Nov. 11, 2004).
[53] LaRaye Brown, *Some Ballots Counted Twice: Discovery Raises Further Doubt About Close Treasurer Race*, NEWS-MESSENGER (Nov. 16, 2004).
[54] Gabrielle Banks, *Scattered Problems Reported with Voting Machines*, PITTSBURGH POST-GAZETTE (Nov. 7, 2006).
[55] *Board Should Hold a Revote for the City*, Editorial, READING EAGLE (July 20, 2005).
[56] John Hilton, *DJ Race Still Up in the Air*, THE SENTINEL (Nov. 11, 2005).
[57] Michael P. Buffer, *Errors Discount Election More*, TIMES LEADER (May 23, 2006).
[58] Robert Behre, *Charleston County Voting Under Way; Ballot Misprint, Machine Quirk Get Attention*, POST & COURIER (Nov. 3, 2006).
[59] Kristy Eppley Rupon, *Counting Error Overstates Votes*, THE STATE (Apr. 29, 2005).
[60] Tom Bower, *Bexar Computer Glitch Delays Counting of Votes*, SAN ANTONIO EXPRESS NEWS (Mar. 10, 2004).
[61] *El Paso's Electronic Voting Machines Have Problems*, KFOX-TV NEWS (Nov. 3, 2006); Vic Kolenc, *Voting Machine Problems Checked*, EL PASO TIMES (Nov. 4, 2006).
[62] *Glitch Forces Manual Tabulation for U.S. House Race*, DALLAS MORNING NEWS (Nov. 8, 2006).
[63] *Jefferson County Voters Continue To Raise Concerns About Voting Machines*, KFDM-TV (Oct. 28, 2006).
[64] Brian Williams, *Software Blamed in Precinct 8 Democratic Chair Race Mixup*, LUBBOCK AVALANCHE-JOURNAL (Mar. 11, 2004).
[65] *Ballot Glitches Reverse Two Election Results*, THE HOUSTON CHRONICLE (Nov. 8, 2002).
[66] Anna M. Tinsley & Anthony Spangler, *Vote Spike Blamed on Program Snafu*, FORT WORTH STAR-TELEGRAM (Mar. 9, 2006); Anna M. Tinsley, *Judicial Candidate Files Challenge*, FORT WORTH STAR-TELEGRAM (Apr. 6, 2006).
[67] Lee Nichols, *County Responds to Voting Machine Problems*, AUSTIN CHRONICLE (Oct. 22, 2004).
[68] David Cho, *Fairfax Judge Orders Logs of Voting Machines Inspected*, WASHINGTON POST (Nov. 6, 2003).
[69] Lauren Glendenning, *Voting Glitch in Fairfax*, CONNECTION NEWSPAPERS (Nov. 8,2006).
[70] *Scattered Reports of Voters Being Blocked and Machine Malfunctions*, KING5.COM (Nov. 2, 2004).
[71] Jake Rigdon, *About 600 Medford Ballots Cast in November Ignored*, MARSHFIELD NEWS-HERALD (Mar. 12, 2004).
[72] Matthew Van Dusen, *Clerk Changes Election Vote Totals*, CASPAR STAR-TRIBUNE (Aug. 21, 2004).

APPENDIX B: SELECTION OF ADDITIONAL PRECINCTS IN CLOSE ELECTIONS

Although we strove to make the discussion in the main text of this report non-technical, some readers might like additional details about the probability models that underlie our discussion of full-precinct audits.

The basic goal in auditing an election is to find any errors or fraud. As a lower bound, an audit must be capable of finding any discrepancies that lead to a change in the outcome of an election. Our model first determines how many precincts must have discrepancies to change the outcome of an election, and then determines how many precincts must be sampled to discover that discrepancy.

A. ESTIMATING THE NUMBER OF DISCREPANT PRECINCTS

The granularity of the audit is a single precinct. To determine the necessary sample, we must first determine the minimum number of precincts that must have error or fraud in order to modify the outcome of the election.

To estimate the number of discrepant precincts:

1. Assume that a switch of more than twenty percent of the votes in any given precinct would be detected without an audit (as previously discussed, *supra* at page 12, this is a common assumption made in academic papers that address post-election audits).

2. Then calculate *b* by assuming that there are just enough discrepant precincts (with no more than twenty percent of any given precinct's votes corrupted, as discussed in step 1) to reverse the unofficial margin of victory. In a simple two-candidate race, a switch of twenty percent of the votes in all precincts in a jurisdiction would swing the margin of victory forty percent. This is the maximum overall vote shift; each precinct would show discrepancies. For example, an election whose actual count is sixty-five percent in favor of Candidate A and thirty-five percent in favor of Candidate B would end up as forty-five percent for A, fifty-five percent for B. Stanislevic provides a formula for calculating *b* for an arbitrary vote-switching maximum as well as an algorithm for calculating *b* when precincts are of different sizes.[1]

In essence, this method specifies the assumed distribution of discrepant precincts that an audit should search for. A race with a relatively narrow margin of victory must be assumed to have few corrupt precincts. Conversely, this method holds that, for a wide-margin race, an audit should be designed to detect a relatively large number of discrepant precincts, because reversing a wide-margin race would require corruption in many precincts.

---

[1] Howard Stanislevic, *Random Auditing of E-Voting Systems: How Much Is Enough?* 9 (version as of Aug. 16, 2006) (Aug. 9, 2006), *available at* http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf.

B. GETTING TO THE "CONFIDENCE LEVEL"

Once we know the minimum number of discrepant precincts for a given margin, the basic question of the post-election audit becomes, "If there are *b* discrepant precincts out of a total of *N* precincts, how many precincts must be sampled to have *x* percent chance of finding at least one of the discrepant precincts?" Note there is a mathematical simplification to discussing detection in terms of finding at least one discrepant precinct, rather than detecting an exact number of discrepant precincts. Since detecting at least one precinct aligns with the practical goals of a post-election audit, this is how we will frame the rest of our discussion.

A probability model, widely known as "sampling without replacement," answers this question exactly. Instead of going through the mathematics involved, and reviewing those exact answers, we describe some general features of this model as applied to the post-election auditing context.

1. **Confidence level:** The chance of finding at least one discrepant precinct (the *x* percent in the question posed above) is commonly referred to as the *confidence level*. For example, an audit that is designed to provide a ninety-five percent chance of finding at least one discrepant precinct is said to have a ninety-five percent confidence level. We are making an assumption about the probability of detection with the audit method. This is not "confidence level" as used in hypothesis testing for statistical significance.

2. **Input:** The formula for sampling without replacement takes the total number of precincts, the number of discrepant or miscounted precincts, and the number of precincts audited (i.e., audit size) as inputs.

3. **Output:** Once the three input variables are specified, the sampling without replacement model reveals the probability of finding a specific number of discrepant precincts.

4. **A few simple rules:**
    a. For a given total number of precincts and a fixed audit size, a greater number of discrepant precincts creates a greater probability that at least one of them will be detected through the audit.

    b. For two jurisdictions with different numbers of precincts, an audit size of the same *percentage* of precincts will have an equal chance of detecting the same *number* of discrepant precincts. Thus, for example, if Jurisdiction A has 100 precincts and Jurisdiction B has 1,000 precincts, a five percent audit of both jurisdictions would have an equal chance of detecting twenty discrepant precincts.

       Note in this example that Jurisdiction A has a discrepancy rate of twenty percent, while the discrepancy rate in Jurisdiction B is two percent; yet a five percent audit of both jurisdictions produces the same probability of detecting at least one discrepant precinct.

c. For a given discrepancy rate (e.g., twenty percent of precincts have discrepancies), a jurisdiction with a small number of precincts must audit a *higher percentage* of its precincts if it is to have the same chance as a larger jurisdiction of detecting at least one discrepant precinct. In terms of the example above, for a discrepancy rate of twenty percent and a ninety-five percent probability of finding at least one discrepant precinct, Jurisdiction A must audit a higher percentage of its precincts than Jurisdiction B.

APPENDIX C: RANDOMNESS SELECTION PROCEDURES

THE ROLE OF DICE IN ELECTION AUDITS – EXTENDED ABSTRACT

Arel Cordero* (arel@cs.berkeley.edu), David Wagner* (daw@cs.berkeley.edu), David Dill† (dill@cs.stanford.edu) (June 16, 2006)

ABSTRACT

Random audits are a powerful technique for statistically verifying that an election was tabulated correctly. Audits are especially useful for checking the correctness of electronic voting machines when used in conjunction with a voter-verified paper audit trail (VVPAT). While laws in many states already require election audits, they generally do not address the procedure for generating the random sample [12]. The sample generation procedure, however, is critical to the security of the audit, and current practices expose a security flaw. This paper examines the problem of sample selection in the context of election audits, identifies necessary requirements for such a procedure, and proposes practical solutions that satisfy those requirements.

1 INTRODUCTION

Many things can go wrong in an election, whether intentionally or unintentionally. The ability to detect (and correct) errors is critical. Recent decades have seen widespread use of computers and automation in elections, including use of optical scan machines, DRE (direct recording electronic) machines, and computerized election management systems to record, tabulate, and report votes. Unfortunately, this trend has come at some cost to transparency, as the automation of these processes reduces opportunities for observers and interested members of the public to monitor the operation of the election. Random audits, performed after the election but before certification, remain as one of the few defenses for ensuring fairness and for building public confidence in the result. Consequently, the details of these audits are of increasing importance to election integrity.

When done right, and in a transparent and publicly observable way, random audits can establish *objective* and *quantifiable* measures of election accuracy.[1] However, without a transparent process, there is no reason to believe an audit will correctly represent the election, which would defeat objectivity, rendering it meaningless as an assurance of fairness. Even if correct, a non-transparent audit would have trouble quelling skepticism and could thereby fail to provide confidence in an election.

All parts of an audit must be performed correctly—and transparently—for the audit to mean anything. In particular, getting the random sample selection process right is critical. To start with, the selection process must ensure every vote has an equal (or minimal) probability of being selected. Moreover, like any fair lottery, a second requirement is that no party be able

* University of California, Berkeley, CA, 94720
† Stanford University, Stanford, CA, 94305

[1] The theory of statistical polling and statistical quality control provides a quantitative measure of confidence in the accuracy of election results, which can be calculated as a function of parameters such as the sample size [9].

to bias or predict the selection in any way. An important implication is: *for an audit to give every party confidence in an election, every party must also have confidence in the fairness of the sample selection.* In other words, sample selection can easily become a weak link in the security of an election.

A case in point is the 2004 U.S. presidential contest in Cleveland, Ohio [8]. Cleveland election workers, in an effort to prevent a complete recount, surreptitiously preselected an audit sample (3% of the total precincts) to ensure the ballots recounted by hand would match the initial machine counts. Then, with public observers present, the workers faked a random selection and the preselected sample was used, defeating the purpose of the audit. Because of this deliberate or negligent action, the true result of the race in Ohio, the deciding state in the presidential race, may never be known. To that extent, the integrity—or security—of the election was compromised.

2 BACKGROUND

In the United States, elections are conducted at a local level [3]. In California, for instance, specifications for equipment are set by Secretary of State and are implemented by counties according to California election code [1]. As residents of Alameda County, California, we have observed the election and audit procedures used there, and we will use California and Alameda County as a running example of current practices.

2.1 CALIFORNIA

California election code has included, for the past four decades, a requirement for a 1% manual tally (or audit) after every election:

> §336.5 "One percent manual tally" is the public process of manually tallying votes in 1 percent of the precincts, selected at random by the elections official, and in one precinct for each race not included in the randomly selected precincts. This procedure is conducted during the official canvass to verify the accuracy of the automated count [2].

The process is *public*, meaning that any citizen is invited to observe every step of the audit. This requires a transparent process. They 1% manual audit is performed as part of the official canvass, as one of the last steps before the final election results are certified. Typically, after the sample is selected, election officials print out a report containing the electronic tallies for just the selected precincts, recount by hand (using three- or four-person recount boards) all the paper ballots cast in each selected polling place, and check to make sure that the manual count in each precinct matches the electronic count in that precinct.

The law requires every county to randomly select a minimum of 1% of precincts for the manual recount, but does not stipulate *how* it should be done. As it happens, Alameda County (Figure 1), and presumably many other counties, have turned to computers to perform the random selection.

Largest Cities	Oakland, Fremont, Hayward, Berkeley
Population	1,507,500
Registered Voters	714,490
Total Voting Precincts	1,140
Absentee Precincts	240

Figure 1: Some basic facts about Alameda County, CA.

3 SAMPLE SELECTION

Computers are generally inappropriate for generating random samples in an election audit. Excellent software-based pseudorandom number generators (PRNGs) exist, so it might not be obvious why this use of computers in *election audits* is inappropriate. The inherent problem is transparency: running software is not observable. In fact, this is the exact problem faced by DREs, and the exact problem election audits, together with voter-verified paper audit trail (VVPAT) systems, intend to address. The use of a computer as a random source jeopardizes the integrity of the audit and election.

One devastating threat is that an insider might be able to tamper with the software used for random selection in a way that allows him or her to know in advance the outcome of the selection. An insider could then use this to cheat without—or with a lesser probability of—getting caught. For instance, an insider with advance knowledge of the selected precincts will be free to defraud all other precincts without fear of detection. Or, if the insider has already tampered with the votes in some precincts, the insider could modify the computer's PRNG to exclude the possibility of choosing those precincts. These attacks could be mounted in a way that is very difficult or impossible for observers to detect. Without a verifiably random sample, it is not clear that such an accusation could be defended against.

Dedicated hardware random number generators (perhaps based on physical phenomena such as radioactive decay, or radio static) are subject to the same transparency problem, despite typically being excellent random number generators. Without transparency, even with a perfect random source, it is hard or impossible to trust the authenticity of its output (Figure 2).

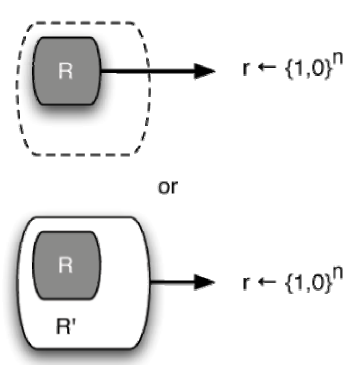


Figure 2: Transparency can be a problem regardless of the quality of the random number generator.

3.1 REQUIREMENTS

As we saw above, "black-box" random sources are a vulnerability for election audits. What requirements must a viable source meet? Many choices exist for generating random numbers; providing them unpredictable—in this case, to *all* parties—is difficult, if even possible [11]. What matters in the election setting, however, is choosing a procedure that can be used, understood, and trusted by an average member of the voting public, for instance, by an average high school graduate.

A transparent procedure for sample selection involves two problems:

1. *Transparently generating random bits*, and

2. *Transparently turning those bits into a sample.*

Technically, this may seem like a trivial distinction. However, the requirements that follow apply equally to both, and especially because the needs of a general audience must be considered, satisfying the requirements for both is not as easy as it might seem. Many natural schemes have non-obvious problems or pitfalls. In the remainder of the section we lay out several requirements for a transparent random source and selection procedure, and subsequently evaluate possible solutions against these requirements.

Simplicity. *The procedure must be simple to follow and execute.* The public must, without extensive education, understand the procedure, why it is fair, and why they should trust it. Otherwise, confidence in the audit and election may be limited. Additionally, complexity introduces opportunities for error or exploitation.

Verifiability. *The procedure must be verifiable either by inspection (i.e., it is physically observable) or by some other property (e.g., cryptography).* Verifiability is imperative. Every observing party must be assured that the selection is genuinely random with a satisfactory distribution. Otherwise, as in Ohio, the audit could be subverted, or observer's confidence undermined.

Robustness. *The distribution of the procedure must be hard to bias or manipulate.* It should be difficult for any party, particularly someone working from the inside, to affect or gain information about what set of ballots is included or excluded from the audit.

Efficiency. *The procedure must not take an incommensurate amount of resources to prepare or execute.* Election worker's and observer's time, energy, money, patience cannot be taken for granted. As the incident in Ohio demonstrated, the cost of time might tempt election workers to fudge the procedure. Or, perhaps, impatience could reduce an observer's vigilance.

4 POSSIBLE RANDOM SOURCES

We first examine the applicability of several random sources to election audits, in light of the requirements above.

Cryptography. From the perspective of a cryptographer, the problem of verifiably-random numbers is (at least in principle) solved. One solution [7], for instance, is to have every observer pick a random number of their own and commit to it, perhaps by writing it down and dropping it in a box. When everyone has committed their numbers, they are revealed and summed modulo some number *N*. The result will be a random number if at least one observer was honest. This could then be built into a very reasonable scheme to perform sample selection.

To an extent, this solution meets all our criteria. However, if we consider trying to explain this to the general public and to election's officials, it might take some work. The concepts of modular arithmetic, independence, and uniformity of distributions must be understood. Also, cryptographic protocols often rely on participants to protect their own interests, which can be a problem when dealing with a non-cryptographer public. For instance, suppose instead of dropping numbers into a box, numbers are written on a board so that the attacker has the "last say," and thus deterministically chooses the outcome. The protocol assumes a savvy enough public to know that commitments are supposed to be hidden.

Drawings. A familiar method of random selection is a drawing in which tickets are mixed then drawn from a hat or box. For instance, we could write all the precincts down on pieces of paper, place them in a box, mix the pieces of paper well, and draw our sample.

Verifiability is difficult when many objects are involved. For instance, if there are 1,000 tickets for 1,000 precincts, every observer must be assured that all precincts are included in the drawing because omissions represent those precincts an attacker could subvert freely. Thus, robustness is an issue as well.

The use of many objects also makes it hard to tell whether they have been adequately mixed. For instance, the Vietnam draft lottery of 1970 used such a scheme, but was later discovered to have suffered from bias: birth-dates later in the year were added last, and due to insufficient mixing, were more likely to be chosen earlier [13].

Lottery-Style Drawings. Lotteries put a great deal of resources and creativity into maintaining secure random number generators. Lottery machines are culturally familiar and trusted to the extent that the lottery is played by millions of people. It would be prohibitively expensive, however, to replicate and maintain a lottery machine in each Registrar of Voters office, so if we were to create a sampling scheme from lottery numbers, we would want to use the same machinery—and perhaps drawings—used for the actual lottery.

Although simplicity, verifiability, and robustness are excellent, efficiency can become a problem and must be carefully considered in any scheme using lottery drawings. For instance, if a state lottery is chosen, this might impose a heavy travel burden on vigilant observers determined to witness the selection. Another issue might arise because U.S. elections are performed locally: if a single dedicated state-wide lottery were used for selection, coordination between county and state might be a problem (e.g., the lottery could only be done when the last county is ready).

Alternatively, the use of an agreed-upon future drawing as input to a deterministic algorithm that creates the sample, might make an excellent scheme. However, the algorithm must also satisfy the requirements in Section 3.1. Particularly, it must be verifiable and understandable to the general public.

Random Number Charts. Another idea might be to use a book filled with random numbers [10] as a basis for selection. Of course, printed books or charts are static documents and must be assumed to be known in advance to any attacker. Consequently, any methods that use books of random numbers would have to find another random method of selecting digits within the documents.

Cards. Cards are a time-tested source of randomness. Indeed, they are used in many high-stakes games. However, there are fifty-two cards in a deck, making it hard to verify—especially when subject to sleights of hand, such as those found in card tricks. As with drawings, it might be difficult to ensure the deck is sufficiently shuffled.

Another issue with cards is that not everyone is familiar with their properties (the suits, the ranks, the number of cards), nor how to handle or shuffle cards well. We would prefer a sample selection scheme that as many people as possible understand and could use.

Depending on how the cards are used, efficiency could also come into play, since every action needs to be observed and verified, and preceded by a shuffle.

Coins and Dice. Coins are the quintessential random number generator and arguably the most ubiquitous. Methods even exist to mitigate any bias in a coin[2]. The primary drawback of coins is that their bandwidth is limited: generating many bits of randomness requires many coin tosses, which takes time.

Dice produce a higher bandwidth of random numbers[3], and are available with different numbers of faces. Ten-sided dice are especially appealing because they map directly onto the decimal numbers. Efficiency can be quite reasonable with dice, especially when multiple dice are rolled at once.

Dice, as with coins, can be biased—intentionally perhaps—so care must be taken to ensure fair dice [5]. Techniques for mitigating potential attacks exist and include: using only new, translucent dice; using a ribbed tumbler to roll the dice; and rolling the dice onto a flat ridged surface such as a dice tray (Figure 3). A dice setup involves the use of few objects, which is good for verification, and dice are simple to understand. They have stood the test of time[4] and are commonly used in games, including high-stakes games. In our proposed solutions that follow we choose dice as the source of randomness primarily because of the simplicity, and the verifiability benefits of using few objects.

---

[2] Assuming independence of coin flips, pairs of flips from the same coin can be used to eliminate any bias the coin may have. If we throw out any HEADS-HEADS or TAILS-TAILS combinations, we are left with two outcomes that bare equal probabilities. This idea is attributed to John von Neumann.

[3] Dice can be considered multi-faced coins.

[4] In fact, dice have existed for thousands of years.

Figure 3: A ten-sided die, tumbler and tray.

Number	*Precinct ID*
0	P_1
1	P_2
⋮	⋮
$N-1$	P_N

Figure 4: A numbered list of precincts.

5 CREATING THE SAMPLE

Once a source of randomness is chosen, a practical procedure must be built around it to perform the sample selection. The procedure, like the random source, must satisfy our above requirements: it must be simple to use and understand, easy to verify, robust against tampering and reasonably efficient.

For schemes we present, we opted for simplicity because that makes the other requirements easier to reason about. While designing a procedure for Alameda County, our initial proposals involved the use of math (not necessarily complex math). However, the feedback we got indicated the less math, the better. We then considered using computers to perform the math during the selection, but our feedback indicated that no reliance on computers was preferable. We also considered creating worksheets, such as tax worksheets, to guide users through the procedure. However, people generally do not enjoy working on taxes, and if people were to find the worksheets inefficient or frustrating, they might elect to fudge or abandon the procedure.

Keeping that in mind, we tried to separate the "work" from the "sheet" by creating pro-computed lookup tables. The procedure we arrived at requires virtually no math to use.

The Basic Idea. We begin by preparing a list (numbered 0, 1, 2, …, $N-1$) of the population we are sampling from. In California, this would involve preparing a list of the names (or IDs) of every precinct to be included in the audit. Numbering each entry sequentially from 0 to $N-1$ establishes a one-to-one mapping of the integers $[0, N-1]$ to the list of precincts (Figure 4). Election officials commit to this ordering before the audit by publishing the list and providing a copy to each political party and each observer. We assume that the audit is not performed until a final electronic tally is available; the goal is to verify whether these alleged election results match the paper records. Election officials commit to the electronic results before the audit by printing the electronic vote totals broken down by precinct, or by writing them onto write-once media (such as CD-ROM), and providing a copy to every interested observer.

Once these preparation steps have been completed, the random selection process begins. In our scheme, an election official rolls an appropriate number of dice to get a random number between 0 and $N-1$, and then uses the one-to-one mapping established earlier to interpret this number as identifying a single precinct. This precinct is added to the random sample, and the process is repeated until the random sample is of the desired size.

If we used standard six-sided dice, rolling k dice would allow us to randomly choose a number between 0 and $6^k - 1$ by reading off the k outcomes and treating them as a number in base-6. However, requiring election officials and observers to perform base-6 arithmetic may be unreasonable. Therefore, instead of using standard dice, we propose using commonly available ten-sided dice[5], letting each die signify a decimal digit. For example, if we want to select one precinct from a list of 1000, we could use three dice to get a number between 0 and 999.

The above procedure handles the case where N is a power of ten. If N is not a power of ten, one simple method is to roll $\lceil \log_{10} N \rceil$ ten-sided dice, and then re-roll if the resulting number is too large. For instance, suppose we want to choose at random from a list of N = 750 precincts. Throwing three dice gives us a random number from 0 to 999. Because only the numbers 0 through 749 correspond to precincts on our list, we ignore and re-roll any time we get a number greater than 749. Because every three-digit number has an equal probability of appearing[6], this method produces a uniform distribution over 750 precincts.

As we have presented it so far, this scheme works reasonably well for a small number of selections, (say $N \leq 1000$). However, re-rolling can become a problem. There is a significant difference between using three dice to select 1% of 1,000 precincts, and using four dice to select 1% of 1,001. Below, we address this issue by using more general range-lookup tables.

5.1 General Dice Scheme

As discussed above, re-rolling can become inefficient quite quickly. To address this, a natural optimization is to divide the range of the dice into N equal intervals, letting each interval correspond to a precinct on the list[7].

For example, suppose we want to use four ten-sided dice to select a precinct from a list of N = 1001 precincts. First we divide the range [0, 9999] into 1,001 equal sized intervals [0, 8], [9, 17], …, [8991, 8999], [9000, 9008]. We then let each *interval* correspond to a precinct on our list, allowing the remainder, [9009, 9999], to correspond to a re-roll. As a result, we throw out roughly 1 out of 10 rolls instead of 9 out of 10, improving efficiency greatly. See Algorithm 1 for a specification of this scheme.

We can simplify the presentation of this scheme by changing how we prepare the numbered list of precincts. Instead of labeling each precinct with an integer, we could label each precinct with its pre-computed range (Figure 5). Now, no arithmetic is necessary to do the selection: one can simply roll k dice and then look up the outcome on the list to obtain a precinct.

---

[5] 10-sided dice can be found at game stores, are often used in board and role-playing games, and typically are numbered 0 through 9.

[6] Subject to any bias present in the random source. If a verifiable and robust source is used, according to our requirements in Section 3.1, this bias is negligible.

[7] We use division, rather than modulo, because division is a more familiar concept to a general audience.

Algorithm 1 General Dice Scheme

INPUTS:
N — number of precincts
n — size of sample
OUTPUTS:
S — set of precincts selected for the sample
ALGORITHM:
$S \leftarrow \emptyset$
$k \leftarrow [\log_{10} N]$
  (k = the number of tosses per selection)
$d \leftarrow [10^k/N]$
while $|S| < n$, do:
    Roll k dice to get a random number
    $x \in \{0, 1, \ldots, 10^k - 1\}$.
    Set $y \leftarrow [x/d]$.
    If $y < N$ and $y \notin S$, then:
        Set $S \leftarrow S \cup \{y\}$.
return S

Numbers	*Precinct ID*
0…8	P_1
9…17	P_2
⋮	⋮
9000…9008	P_{1001}
9009…9999	RE-ROLL

Figure 5: A list of 1001 precincts labeled with equal-sized ranges.

5.2 ANALYSIS

It should first be noted that this simple idea of using range-lookup tables applies to other random sources, and can enable other nice things like allowing for a controlled bias (say to account for precinct sizes).

Advantages. The foremost advantage of this scheme over computer-based PRNGs is the use of an observable random source. Dice are simple, robust and familiar enough to be widely accepted.[8]. Dividing up the range of the dice improves efficiency while maintaining simplicity. The efficiency and usability of this scheme is excellent. As shown in Figure 6, election officials can easily select a random sample of 1% of the precincts, and even very large counties will not need too many tosses of the dice. For instance, even with $N = 2000$, only about 25 tosses of the dice (on average) are needed to select a random 1% sample. This fairness of the scheme is also verifiable (to the extent that dice are) because the lookup table is published; it can be inspected after the fact to verify that, for example, every precinct was included and had an equal chance of being selected.

Disadvantages. When the size of the sample is a large ratio of the population, many more re-rolls would be expected, as "collisions" occur in the sample selection. For small ratios this loss is negligible.

Unfortunately, the cost of this scheme scales linearly (keeping the sample to population ratio constant) with the size of the sample. While this might be suitable for selecting 1% of 500 or 1,000 precincts, it might be too time consuming to select 1% of 1,000,000.

[8] The proposal to use dice was met with enthusiasm from election officials in Alameda County.

A second concern is the threat of biased dice. If a malicious party were able to affect the distributions of the dice (say by weighting a die or by swapping in a die with duplicate faces), that party could affect which precincts get selected, or worse, which precincts *do not* get selected.

Efficiency. In an election setting, dice not only have to be rolled, but inspected by observers. This incurs a cost per roll, so we measure the efficiency of our methods by the number of rolls they require.

We can partially reduce this cost by rolling multiple dice at once. If we do this, we must ensure the order of dice is well-specified in advance. One idea is to use dice with different magnitudes on their faces, such as 1's, 10's, and 100's. Another possibility is to use dice of different colors and establish a clear ordering of the colors before rolling the dice. A good choice in the United States would be red, white and blue for their culturally meaningful order. This would enable us to roll three dice (one red, one white, and one blue) at a time; for instance, if the red one comes up 5, the white one 7, and the blue one 2, that would be interpreted as the three-digit number 572.

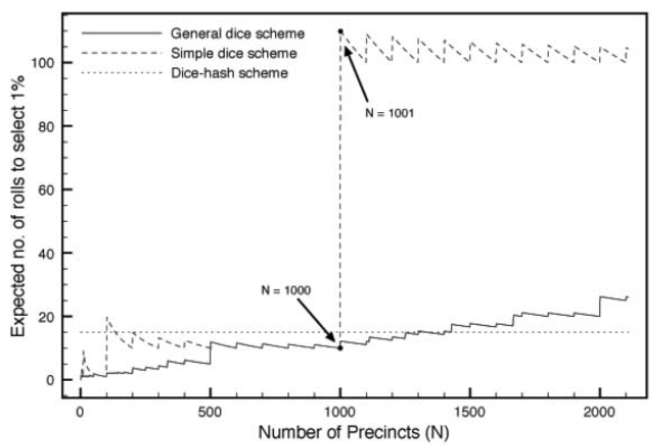


Figure 6: The expected number of tosses of 10-sided dice to select a 1% sample using range-lookup tables (General dice scheme) versus simply re-rolling (Simple dice scheme) as a function of population size (*N*). The Dice-hash scheme is a deterministic function, similar to [4], to calculate a sample selection using a constant number of dice rolls as input.

6 RELATED WORK

The idea of using auditing to gain statistical confidence in an election is not new. Many states, such as California, already require random audits or manual tallies in their election codes.

Prior work has looked at the issue of the statistical validity of random audits and what size sample is necessary to achieve a given degree of confidence [9]. In these papers, however, the sample selection process is not considered and is assumed to be perfect. Some authors have examined the possibility of auditing individual ballots, stating that if adopted (in a privacy-preserving way), audits of individual ballots could give much higher degrees of confidence with less overall counting [6, 9].

Other people have looked at verifiable methods of sample selection. The IETF uses an algorithm based on cryptographically strong hash-function, to expand input from a random source into a sample [4]. In the full version of this paper we present a similar scheme, and address its viability in an election setting. Some initial reactions, however, indicated resistance and skepticism from people unfamiliar with hash functions and cryptography, leading us to prefer a dice-only approach.

7 CONTRIBUTIONS

Sample selection is a critical part of an audit, but has been overlooked in the election setting, as evidenced by the wordings of election code [12], and existing current practices such as the use of software-based PRNGs. We identify non-transparency as a vulnerability for every part of an audit, particularly sample selection, and lay out requirements that a transparent sample selection procedure must meet.

In addition, we present an algorithm and implementation for transparent sample selection, using dice and a printed lookup table. This scheme is simple and relatively efficient, no calculations are needed to perform the selection, and, if adopted, would make elections more trustworthy.

8 CONCLUSION

Transparency plays an important role in the security of election audits. Because auditing is a public process capable of establishing confidence in an election's outcome, it is critical that every part of the process, particularly the random sample selection, be transparent, observable, and understandable to all interested parties. While the current use of computers to generate samples is neither transparent nor observable, we have presented a possible remedy that is simple, verifiable, low-cost, and robust.

Ultimately, it is essential that we choose random audit procedures that are capable of convincing the whole population of the genuineness of the audit, and, in turn, of the election.

9 ACKNOWLEDGMENTS

We would like to express our deep gratitude for the Alameda County Registrar of Voters office for the generous time and effort they have provided to help us better understand the process of voting in California. In addition we would like to thank the many people who contributed to this discussion of random sample selection in person and by e-mail.

REFERENCES

[1] California Elections Code, 1965. Section 19201.
[2] California Elections Code, 1965. Section 336.5.
[3] United States Elections 2004, 2004. http://usinfo.state.gov/products/pubs/election04/procedure.htm.
[4] D. Eastlake. Publicly Verifiable Nominations Committee (NomCom) Random Selection, June 2004. RFC 3797.
[5] Encyclopaedia Britannica. Dice, April 2006. Encyclopaedia Britannica Premium Service.
[6] K. C. Johnson. Election Certification by Statistical Audit of Voter-Verified Paper Ballots, October 2004. Available at SSRN: http://ssrn.com/abstract=640943.
[7] J. Killian. *Uses of Randomness in Algorithms and Protocols*. MIT Press, 1990.
[8] J. Mazzolini. Workers Accused of Fudging '04 Recount. The Cleveland Plain Dealer, 4 2006.
[9] C. A. Neff. Election Confidence. Manuscript, 2003.
[10] Rand Corporation, editor. *A Million Random Digits with 100,000 Normal Deviates*. Rand Corporation, 1955.
[11] B. Schneier. *Applied Cryptography*. John Wiley & Sons, Inc., 2nd edition, 1996.
[12] P. Smith and B. Kibrick. Manual Audit Requirements. Verified Voting Foundation, September 2005.
[13] N. Starr. Nonrandom Risk: The 1970 Draft Lottery. *Journal of Statistics Education*, 5(2), 1997.

THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

Lawrence Norden *et al.* (Brennan Center for Justice ed., 2006)

APPENDIX F: EXAMPLE OF TRANSPARENT RANDOM SELECTION PROCESSES

A transparent random selection is one where members of the public can verify that, at the time of the choice, all selections were equally probable. Here are two examples of (reasonably) transparent random choice methods. There are many variations on these methods.

Method A: Each member of a group of individuals representing diverse interests chooses a random number (by any method) in a specified range 1…*N* and writes it down on a slip of paper. After each participant has chosen a number, the numbers are revealed to all and added. They are then divided by *N*, and the "integer remainder" is the number that is chosen (this is known in mathematics as the "modulo").

The best way to understand this is by example. Little Pennasota County has 9 machines (labeled "1" through "9") and wants to select one of these machines to Parallel Test. They want to ensure that the machine is chosen at random. To do this, they bring together several participants: a member of the League of Women Voters, the Democratic-Republicans, the Federalists, the Green Party, and the Libertarian Party. Each person is asked to select a number. The League of Women Voters' representative selects the number 5, the Democratic-Republican chooses 6, the Federalist chooses 9, the Green chooses 8 and the Libertarian chooses 9. These numbers are then revealed and added: 5+6+9+8+9=37. They are then divided by 9. The "integer remainder" is 1, because 37 is divisible by 9 four times, with an integer remainder of 1 (or, 36 + 1). In this scenario, machine number 1 is chosen.

Any member of the group can assure the result is not "fixed" by the others. In the example above, all of the political parties might want to conspire to ensure that machine number 2 is picked for Parallel Testing. However, the League of Women Voters representative will prevent them from being able to do this: without knowing what number she is going to pick, they cannot know what the integer remainder will be.

Method B: Color-coded, transparent 10-sided dice are rolled (in a dice cup) in public view. The digits on the top faces of the dice are read off in a fixed order determined by the colors (e.g., first red, then white, then blue). This yields a random 3-digit number. If the number is out of the desired range, it is discarded and the method performed again**.**

Note about transparently random selection process: For a transparently random selection process to work, (1) how the randomly selected number is going to be used must be clearly stated in advance (i.e., if we are choosing a number to decide which machine to Parallel Test, each machine must be labeled with one of the numbers that may be chosen), (2) the process for randomly selecting numbers must be understood by all participants, and (3) the event of randomly selecting numbers must be observable to all participants (and, if possible, members of the public).

For example, if we are picking what team of police are going to be left to look after the locked-up and security-sealed election materials before completion of the Automatic Routine Audit, the observers and participants must see the committed list of police that are being selected from in advance of the selection. The list must be posted visibly or in some other way "committed to" so that the association between random numbers selected and people selected cannot be switched after the numbers are produced.

In terms of assigning auditors to roles and machines to be audited, the goal might be to make sure that there is one Democratic-Republican and one Federalist assigned to review the paper records (the readers) and one Democratic-Republican and one Federalist assigned to tally the records (the writers). There should be no way to know what machines anyone will be assigned to, nor who will be teamed with whom during the audit.

If the use or interpretation of the random numbers is not clear and committed in advance, then an appropriately situated attacker might "interpret" the random number in a way that allows the attack go undetected by, for example, assigning attackers as auditors for all the subverted machines.[1]

[1] The importance of making sure that observer/participant understand how the random numbers are to be used is amusingly illustrated in the magic special: Penn & Teller: Off the Deep End (NBC television broadcast, Nov 13th, 2005). In this program an unsuspecting individual is fooled into thinking that the magicians could figure out in advance what card he or she will select because, no matter what card is selected, the magicians can point to its representation somewhere on the beach. The humorous approach here is that all 52 playing cards were set up in interesting ways on the beach to be revealed. A magician opened his coat for one card, two kids in the water held up their rafts to form a card, a sunbather turned around with a card painted on her back, cards were found inside of a potted plant and coconut, etc.

ENDNOTES

[1] VerifiedVoting.org, *Mandatory Manual Audits of Voter-Verifiable Paper Records, available at* http://www.verifiedvoting.org (last visited June 15, 2007).
[2] *Id.*
[3] These states include Georgia, Maryland, Missouri, Pennsylvania, Texas, and Virginia.
[4] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD 121 (Brennan Center for Justice ed., 2006), *available at* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=36343&init_key=105.
[5] *See* Andrew W. Appel, *Effective Audit Policy for Voter-Verified Paper Ballots in New Jersey* (Mar. 9, 2007), *available at* http://www.cs.princeton.edu/~appel/spapers/appel-nj-audits.pdf; Arel Cordero, David Wagner & David Dill, *The Role of Dice in Election Audits – Extended Abstract*, IAVOSS Workshop on Trustworthy Elections (WOTE 2006) (June 29, 2006), *available at* http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf; Kathy Dopp, *How Can Independent Paper Audits Detect and Correct Vote Miscounts?* (version as of July 25, 2006) (June 30, 2006), *available at* http://electionarchive.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf; Kathy Dopp & Frank Stenger, *The Election Integrity Audit* (version as of Sept. 25, 2006), *available at* http://electionarchive.org/ucvAnalysis/US/paper-audits/ElectionIntegrityAudit.pdf (a computer program developed by Frank Stenger and Kathy Dopp for calculating audit details is available at http://electionarchive.org/auditcalculator/eic.cgi); Jerry Lobdill, *Considering Vote Count Distribution in Designing Election Audits* (version as of Nov. 26, 2006) (Oct. 9, 2006), *available at* http://vote.nist.gov/Considering-Vote-Count-Distribution-in-Designing-Election-Audits-Rev-2-11-26-06.pdf; Jerry Lobdill, *Election Audit Sampling Plan – It's Not Just About Sampling Without Replacement* (Oct. 9, 2006), *available at* http://vote.nist.gov/Election-Audit-Sampling-Plan-Design-Its-Not-Just-About-Sampling-Without-Replacement-10-09-06.pdf; Norden *et al.*, *supra* note 2; Ronald Rivest, *On Auditing Elections When Precincts Have Different Sizes* (version as of Apr. 29, 2007), *available at* http://people.csail.mit.edu/rivest/Rivest-OnAuditingElectionWhenPrecinctsHaveDifferentSizes.pdf [hereinafter Rivest, *On Auditing*]; Ronald Rivest, *On Estimating the Size of a Statistical Audit* (version as of Nov. 14, 2006) (Sept. 19, 2006), *available at* http://people.csail.mit.edu/rivest/Rivest-OnEstimatingTheSizeOfAStatisticalAudit.pdf (Howard Stanislevic has developed a computer program for calculating Rivest's equation at: http://mysite.verizon.net/evoter/AuditCalc.htm) [hereinafter Rivest, *On Estimating*]; Jonathan D. Simon, JD & Bruce O'Dell, *An End to "Faith-Based" Voting: Universal Precinct-Based Handcount Sampling to Check Computerized Vote Counts in Federal and Statewide Elections*, Election Defense Alliance (Sept. 8, 2006), *available at* http://electiondefensealliance.org/files/UPSEndFaithBasedVoting.pdf; Howard Stanislevic, *Random Auditing of E-Voting Systems: How Much Is Enough?* (version as of Aug. 16, 2006) (Aug. 9, 2006), *available at* http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf; Ellen Theisen, *Auditing Election Equipment – The Real Scoop!* (Aug. 27, 2005), *available at* http://www.votersunite.org/info/auditingissues.pdf (movie available at: http://homepage.mac.com/sheltonlankford/.Public/RandomSample.mov; excel spreadsheet available at: http://www.votersunite.org/info/AuditEffectivenessCalculator.xls); *The Titanium Standard for Election Verification and Security* (Oct. 1, 2006), *available at* http://www.velvetrevolution.us/titanium.pdf; Joseph A. Calandrino, J. Alex Halderman & Edward W. Felten, *Machine-Assisted Election Auditing*, 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (forthcoming Aug. 2007), *available at* http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf; Stephen N. Goggin & Michael D. Byrne, *An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots*, 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (forthcoming Aug. 2007), *available at* http://www.usenix.org/events/evt07/tech/full_papers/goggin/goggin.pdf; John McCarthy, Howard Stanislevic, Mark Lindeman, Arlene Ash, Vittorio Addoria & Mary Batcher, *Percentage-Based Versus S.A.F.E. Vote Tabulation Auditing: A Graphic Comparison* (July 26, 2007), *available at* http://www.verifiedvotingfoundation.org/auditcomparison.
[6] *Election Audits: Hearing Before the Subcomm. on Elections of the H. Comm. on H. Admin.*, 110th Cong. (2007) [hereinafter *Election Audits Hearing*].
[7] *See, e.g.*, Simon & O'Dell, *supra* note 5; Stanislevic, *supra* note 5.
[8] Legislation introduced in 2007 to amend or introduce post-election audit requirements include: H.B. 537, 2007 LEG., REG. SESS. (Fla. 2007). H.B. 53, 2007 LEG., REG. SESS. (Pa. 2007), and H.B. 671, 185TH GEN. COURT, REG. SESS. (Mass. 2007).
[9] VerifiedVoting.org, *supra* note 1.

[10] *Collaborative Public Audit of the November 2006 General Election*, The Cuyahoga County Collaborative Audit Committee & Cleveland State University Center for Election Integrity (Apr. 18, 2007), *available at* http://urban.csuohio.edu/cei/public_monitor/cuyahoga_2006_audit_rpt.pdf.
[11] This is sometimes described as "confirm that the right candidate was declared the winner," though this is probably more than any statistical audit can guarantee.
[12] Election Data Services, Inc., *Final Report of the 2004 Election Day Survey* (submitted to the U.S. Election Assistance Commission), 4-7 (Sept. 27, 2005), *available at* http://www.eac.gov/election_survey_2004/pdf/EDS-Full_Report_wTables.pdf.
[13] For instance, in statewide elections in Ohio, the Secretary of State shall order a recount when the vote total of the winning candidate is less than the vote total for the second-place candidate by less than one quarter of one percent. OHIO REV. CODE § 3515.011 (2007).
[14] *See e.g.*, S. 507, 212TH LEG., REG. SESS. (NJ 2007); Dopp, *supra* note 5; Lobdill, *supra* note 5; Rivest, *On Auditing*, *supra* note 5; Rivest, *On Estimating*, *supra* note 5; McCarthy *et al.*, *supra* note 5.
[15] Simon & O'Dell, *supra* note 5.
[16] electionline.org, *Case Study: Auditing the Vote* 5 (Mar. 2007 Briefing), *available at* http://www.electionline.org/Portals/1/Publications/EB17.pdf.
[17] HAW. REV. STAT. § 16-42(b)(3) (2006).
[18] MINN. STAT. § 206.89 (2007).
[19] Stanislevic, *supra* note 5, at 15.
[20] N.Y. ELEC. LAW § 9-211 (McKinney 2007).
[21] CONN. GEN. STAT. ANN. § 9-242b(5) (2007); 10 ILL. COMP. STAT. § 5/24C-15 (2007); E-mail from Dean Logan, Chief Deputy Registrar-Recorder/County Clerk, Los Angeles County, California to Lawrence Norden (Mar. 19, 2007) (on file with the authors).
[22] N.M. STAT. § 1-14-13.1(A) (2007); Telephone interview with Scott Nago, Counting Center Operations Coordinator, Office of Elections, Hawaii (July 1, 2007).
[23] ARIZ. REV. STAT. § 16-602(C) (2007).
[24] CAL. ELEC. CODE § 15630, 19253 (2007).
[25] 10 ILL. COMP. STAT. § 5/24C-15 (2007).
[26] This statement is subject to the caveat that a state recount law might require a full recount in the event of a close election; but this is a possible expense regardless of whether there is a mandatory audit at all.
[27] *See, e.g.*, Dopp, *supra* note 5; Rivest, *On Auditing*, *supra* note 5; Simon & O'Dell, *supra* note 5; Stanislevic, *supra* note 5; McCarthy *et al.*, *supra* note 5.
[28] Dopp, *supra* note 5 (assuming that a corruption of more than fifteen percent of ballots would be caught); Norden *et al.*, *supra* note 4 (assuming that a corruption of more than twenty percent of ballots would be caught); Stanislevic, *supra* note 5 (assuming that a corruption of more than twenty percent of ballots would be caught); McCarthy *et al.*, *supra* note 5 (assuming that a corruption of more than twenty percent of ballots would be caught).
[29] Rivest, *On Auditing*, *supra* note 5; Stanislevic, *supra* note 5.
[30] Appel, *supra* note 5; *See Election Audits Hearing*, *supra* note 6 (Written Statement of Lawrence Norden, Counsel, Brennan Center for Justice at NYU School of Law), *available at* http://www.brennancenter.org/dynamic/subpages/download_file_48698.pdf.
[31] *See, e.g.*, California Department of Industrial Relations, Division of Workers' Compensation, *1994 Audit of Workers' Compensation Insurers, Self-Insured Employers, and Third-Party Administrators* (Mar. 29, 1995), *available at* http://www.dwc.ca.gov/dwc/1994REP1.HTM; Massachusetts Department of Environmental Protection, *Audits Fact Sheet*, *available at* http://www.mass.gov/dep/cleanup/audfs.htm (last visited June 27, 2007).
[32] N.H. REV. STAT. § 660:2 (2007); S.D. CODIFIED LAWS §§ 12-21-8–12-21-11 (2006).
[33] CONN. GEN. STAT. § 9-311a (2007).
[34] ARIZ. REV. STAT. § 16-661(A) (2007).
[35] electionline.org, *supra* note 16, at 5.
[36] HAW. REV. STAT. § 16-42(b)(4) (2006).
[37] MINN. STAT. § 206.89 (2007)
[38] N.M. STAT. § 1-14-13.1(B) (2007).
[39] ARIZ. REV. STAT. § 16-602(D) (2007).
[40] Norden *et al.*, *supra* note 4.
[41] We make a number of recommendations as to what such procedures and laws might look like in *The Machinery of Democracy: Protecting Elections in An Electronic World*, Appendix M at page 147.

[42] MINN. STAT. § 206.57, 66 (2007).
[43] 10 ILL. COMP. STAT. § 5/24C-15 (2007).
[44] Telephone interview with Debra Nieto, Voter Registration and Operations, Office of the County Clerk, Lake County, Illinois (Mar. 19, 2007); Telephone interview with the Office of the County Clerk, Sangamon County, Illinois (Mar. 19, 2007); Telephone interview with Tom Bride, Election Administrator, Office of the County Clerk, Peoria County, Illinois (Mar. 19, 2007); Telephone interview with Doreen Nelson, Assistant Executive Director, DuPage County Election Commission, DuPage County, Illinois (Mar. 19, 2007); Telephone interview with the Office of the County Clerk, Cook County, Illinois (Mar. 21, 2007).
[45] Telephone interview with Scott Nago, *supra* note 22.
[46] Telephone interview with Harvard L. Lomax, Registrar of Voters, Clark County, Nevada (Dec. 12, 2005).
[47] E-mail from Dean Logan, *supra* note 21.
[48] Telephone interview with Scott Nago, *supra* note 22.
[49] Public Meeting, Post Election Audit Standards Working Group, California Secretary of State (July 2, 2007) (Testimony of Deborah Seiler, Elections Manager, Solano County, California; Testimony of John Tuteur, Clerk, Napa County, California) *available at* http://www.sos.ca.gov/elections/post_e/post_election_meet07.htm (last visited July 23, 2007).
[50] E-mail from Anthony Stevens, Assistant Secretary of State, New Hampshire to Lawrence Norden (June 5, 2007) (on file with the authors).
[51] North Carolina State Board of Elections, Statewide May 2006 Primary Election One-Race Audit Results, *available at* http://www.ncvoter.net/downloads/NCSBOE_Primary_Sample_audit_count_short.xls (last visited June 20, 2007).
[52] E-mail from Mark Halvorson, Director and Co-Founder, Citizens for Election Integrity, Minnesota to Lawrence Norden (Feb. 12, 2007) (on file with the authors).
[53] Division of Elections, Pima County, Arizona, *2006 Pima County General Election Audit Summary* (Nov. 29, 2006), *available at* http://www.azsos.gov/election/2006/general/handcount/Hand_Count_06_General_Pima.pdf.
[54] E-mail from Anthony Stevens, *supra* note 50.
[55] At least two people count the same paper record in Clark County, Nevada. Telephone interview with Harvard L. Lomax, Registrar of Voters, Clark County, Nevada (Mar. 23, 2006). A number of counties in California also conduct audits in this manner.
[56] Author Joseph Lorenzo Hall and members of the NSF ACCURATE center are involved in a project to develop detailed procedures for post-election manual tallying with San Mateo and Yolo counties in California.
[57] One Percent Manual Tally Procedures for the November 2006 Election in San Mateo County, California (on file with the authors).
[58] MINN. STAT. § 204C.21 (2007).
[59] The piling method of counting ballots is commended by Citizens for Election Integrity Minnesota. Mark Halvorson & Laura Wolff, *Report and Analysis of the 2006 Post-Election Audit of Minnesota's Voting Systems* 6 (Apr. 4, 2007), *available at* http://www.ceimn.org/files/CEIMNAuditReport.pdf.
[60] electionline.org, *supra* note 16, at 5.
[61] David Wagner, *Thoughts on the Nov. 16, 2006 1% Manual Tally in Yolo County* (Nov. 25, 2006), *available at* http://www.yoloelections.org/news/snews/reactions.pdf.
[62] Stephen Manning, *Paper Jams Hamper Electronic Voting*, ASSOCIATED PRESS (Dec. 21, 2006).
[63] Norden *et al.*, *supra* note 4, at 70.
[64] For a basic primer on the mathematics of post-election audit sampling, *see* Joseph Lorenzo Hall, *A Quick Primer on the Mathematics of Post-Election Audit Confidence* (Mar. 20, 2007), *available at* http://www.josephhall.org/eamath/eamath.pdf.
[65] S. 507, 212TH LEG., REG. SESS. (NJ 2007).
[66] *See* http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00811:.
[67] McCarthy *et al.*, *supra* note 5. Authors define statistical power as "the probability of detecting an outcome-altering miscount – which could occur either accidentally or intentionally."
[68] New Hampshire, where the number of registered voters in a precinct can vary from one to 19,000 voters, provides an extreme example of precinct size variation. Anthony Stevens, Assistant Secretary of State of New Hampshire, Address to Democracy Fest Annual National Convention: Hand Counting Paper Ballots (June 10, 2007) (presentation is available at http://www.democracyfornewhampshire.com/files/Hand_count_training_D-fest_July_5_2007.pdf).
[69] *See, e.g.*, Rivest, *On Auditing*, *supra* note 5; Stanislevic, *supra* note 5.

[70] This calculation assumes that costs of increased audits increased linearly with audit percentage.
[71] *See* Stanislevic, *supra* note 5.
[72] The basic mathematics behind this calculation are covered in Hall's primer. *See* Hall, *supra* note 62.
[73] McCarthy *et al.*, *supra* note 5.
[74] Halvorson & Wolff, *supra* note 59, at 3.
[75] Still, it is worth noting that the Holt Bill allows states to use audits that are "at least as effective" as the scheme proposed in the bill. Thus, a state could probably choose to adopt something close to the adjustable-percentage audit method in its pure form. H.R. 811, 110TH CONG. § 5 (2007). *But see* the main text for reasons that a fixed-percentage minimum audit may be desirable, even if the margin of victory is very large.
[76] Simon & O'Dell, *supra* note 5.
[77] *Id.*
[78] A slightly more complex method – but one that obviates stamping each ballot – is to stack the ballots in a systematic fashion. For example, the ballots could be separated into 100-ballot piles. For each pile, poll workers would place the first ten ballots in "portrait" orientation. The next ten would be in "landscape" orientation. By repeating this pattern for the rest of the 100-ballot pile, poll workers would create a pile in which it is easy to identify any ballot with a number between 1 and 100. Additional 100-ballot piles would contain ballots 101-200, 201-300, etc. It is unclear whether this method would save time compared to the sequential labeling method discussed in the main text.
[79] Simon and O'Dell suggest that the easiest way around this difficulty is simply to replace DREs with other voting systems. Simon & O'Dell, *supra* note 5, at 5-6.
[80] Simon and O'Dell do not address precinct-level tabulation.
[81] Simon & O'Dell, *supra* note 5, at 7.
[82] *See* Simon & O'Dell, *supra* note 5, at 3 n.5.
[83] Note: for large precincts, this might require upwards of 100 rolls of the dice (assuming a ten percent audit in a precinct with 1,000 ballots cast). A reasonable modification would be to roll two ten-sided dice 1/10 as many times and select each corresponding ballot from each stack. *See* Cordero *et al.*, *supra* note 5.
[84] VerifiedVoting.org, *supra* note 1.
[85] electionline.org, *supra* note 16, at 5.
[86] *Id.*
[87] Norden *et al., supra* note 4.
[88] Cordero *et al.*, *supra* note 5.
[89] *Id.*; Norden *et al.*, *supra* note 4.
[90] ARIZ. REV. STAT. § 16-602(C) (2007); 2007 ARIZ. LEGIS. SERV. 295 (West) (pending legislation to update audit requirement); MINN. STAT. § 206.89 (2007).
[91] COLO. REV. STAT. § 1-7-514(1)(a)(I) (2007); N.M. STAT. § 1-14-13.1(A) (2007); WASH. REV. CODE § 29A.60.185 (2007); W.VA. CODE § 3-4A-28(d) (2007).
[92] N.Y. ELEC. LAW § 9-211(1) (McKinney 2007).
[93] CONN. GEN. STAT. § 9-242b(5) (2007).
[94] 10 ILL. COMP. STAT. § 5/24C-15 (2007).
[95] CAL. ELEC. CODE § 15360(d) (2007).
[96] CAL. ELEC. CODE § 15360(c) (2007).
[97] ALASKA STAT. § 15.15.420 (2006); WASH. REV. CODE § 29A.60.185 (2007).
[98] COLO. REV. STAT. § 1-7-514(1)(a)(I) (2007); MINN. STAT. § 206.89 (2007).
[99] ARIZ. REV. STAT. § 16-602(J) (2007).
[100] N.M. STAT. § 1-14-13.1(A) (2007).
[101] Ted Selker & Sharon Cohen, *An Active Approach to Voting Verification*, CalTech/MIT Voting Technology Project Working Paper #28 at 2 (May 2005), *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp28.pdf.
[102] Norden *et al., supra* note 4, at 70. If twenty percent of voters thoroughly check their paper records and notice errors on them, there would be an unusually high number of cancellations.
[103] *See, e.g.*, Frank Stanfield, *Murder and Politics Stir Lake's Year; The Schools' Financial Chaos Ricocheted Through the County, Hurting Reputations and Eliminating Jobs*, ORLANDO SENTINEL, Lake Sentinel Section at 1 (Jan. 1, 2001) (reporting that "a post-election count showed that Vice President Al Gore could have picked up 130 votes in Lake, had the canvassing board counted ballots where voters filled a circle with a pencil and also wrote in the same candidate's name in a space set aside for write-in candidates"); Scott Shuger, *Air Apparent?*, SLATE (Dec.

20, 2000) (reporting that the Orlando Sentinel's examination of 6,000 disallowed Lake County ballots found 376 overvotes, which, if counted, would have given Gore a net 130-vote increase in that county).

[104] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY, AND COST (Brennan Center for Justice ed., 2006), *available at* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=38150&proj_key=76; Michael Tomz & Robert P. Van Houweling, *How Does Voting Equipment Affect the Racial Gap in Voided Ballots*, AMERICAN JOURNAL OF POLITICAL SCIENCE (Jan. 2003), *available at* http://www.stanford.edu/~tomz/pubs/ajps03.pdf.

[105] Norden *et al., supra* note 4, at 81.

[106] Halvorson & Wolff, *supra* note 59, at 5.

[107] *Id.*

[108] William D. Kalsbeek & Lei Zhang, *An Assessment of the May 2006 Election Recount and a Proposed Permanent Recount Sample Design*, Technical Report of the University of North Carolina at Chapel Hill, School of Public Health's Survey Research Unit (July 17, 2006) (on file with the authors) [hereinafter Kalsbeek & Zhang, *Assessment of the May 2006 Election Recount*]; William D. Kalsbeek & Lei Zhang, *An Assessment of the November 2006 Election Recount*, Technical Report of the University of North Carolina at Chapel Hill, School of Public Health's Survey Research Unit (May 25, 2007) (on file with the authors).

[109] electionline.org, *Early and Absentee Voting Laws* (as of 7/26/06), at http://www.electionline.org/Default.aspx?tabid=474 (last visited May 30, 2007).

[110] Election Data Services, Inc., *supra* note 12.

[111] electionline.org, *supra* note 107.

[112] electionline.org, *Provisional Ballot Verification* (updated 8/2/06), at http://www.electionline.org/Default.aspx?tabid=1113 (last visited May 30, 2007).

[113] CAL. ELEC. CODE § 15360(b) (2007); N.M. STAT. § 1-14-13.1(A) (2007).

[114] ARIZ. REV. STAT. § 16-602(G) (2007).

[115] ARIZ. REV. STAT. § 16-602(C) (2007).

[116] ARIZ. REV. STAT. § 16-602(I) (2007).

[117] N.M. STAT. § 1-13-22 (2007).

[118] CAL. ELEC. CODE § 15201 (2007).

[119] CAL. ELEC. CODE § 14434 (2007).

[120] COLO. REV. STAT. § 1-7-505(2) (2007); HAW. REV. STAT. § 11-154 (2006).

[121] COLO. REV. STAT. § 1-7-507(7) (2007).

[122] CONN. GEN. STAT. § 9-266 (2007).

[123] MINN. STAT. § 204C.28 (2007).

[124] WASH. REV. CODE § 29A.44.050 (2007).

[125] WASH. REV. CODE § 29A.60.110 (2007).

[126] *See, e.g.*, Anna M. Tinsley & Anthony Spangler, *Vote Spike Blamed on Program Snafu*, FORT WORTH STAR-TELEGRAM (Mar. 9, 2006) (noting that a programming error in the tally server software caused an extra 100,000 votes to be initially recorded in Tarrant County, Texas).

[127] Kalsbeek & Zhang, *Assessment of the May 2006 Election Recount*, *supra* note 108.

[128] Stephen Ansolabehere & Andrew Reeves, *Using Recounts to Measure the Accuracy of Vote Tabulations: Evidence from New Hampshire Elections 1946-2002*, CalTech/MIT Voting Technology Project Working Paper #11 (Jan. 2004), *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp11.pdf.

[129] R. Michael Alvarez, Jonathan N. Katz & Sarah A. Hill, *Machines Versus Humans: The Counting and Recounting of Pre-Scored Punchcard Ballots*, CalTech/MIT Voting Technology Project Working Paper #32 (Sept. 2005), *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp32.pdf; *See* Kalsbeek & Zhang, *Assessment of the May 2006 Election Recount*, *supra* note 108.

[130] Goggin & Byrne, *supra* note 5.

[131] Calandrino *et al.*, *supra* note 5.

[132] Some of the definitions in this glossary were borrowed from Douglas Jones's "Testing Voting Systems," part of his Voting and Elections webpages, which can be found at http://www.cs.uiowa.edu/~jones/voting/testing.shtml (last visited July 1, 2007).

[133] Norden *et al.*, *supra* note 4, at 121.

[134] McCarthy *et al.*, *supra* note 5.

[135] Norden *et al.*, *supra* note 4, at 125.

BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
212.998.6730 Fax 212.995.4550
www.brennancenter.org

SAMUELSON | Law, Technology & Public Policy Clinic

Samuelson Law, Technology & Public Policy Clinic
at the University of California, Berkeley School of Law (Boalt Hall)

University of California, Berkeley
School of Law (Boalt Hall)
Berkeley, CA 94720
www.samuelsonclinic.org