

Checking election outcome accuracy Post-election auditing procedures

©2010 Kathy Dopp
Ph.D. Student

Rockefeller College of Public Affairs and Policy
State University of New York at Albany
kathy.dopp@gmail.com

Christopher N. Lawrence
Assistant Professor of Political Science
Texas A&M International University
c.n.lawrence@gmail.com

August 2010

Abstract

Current voting systems and procedures used to conduct post-election audits fail to reliably assure the accuracy of election results. Several methods have been found that overcome obstacles to auditing caused by various election system designs. This article provides an overview of the scope and content of post-election auditing practices that are indispensable to ensuring election audits will effectively and reliably check the accuracy of officially-reported election results.

Introduction

Election results can have dramatic effects on the future course of government, whether at the national, state, or local levels. Given the extensive powers of elected officials to influence society—from matters of war and peace, to the appropriation of large sums of money for preferred projects and programs—it is not surprising that attempts to corrupt the electoral process to gain unearned victories at the ballot box have been widespread in history.

Over time, in the United States there has been a considerable effort to stamp out corruption in ballot counting. However, the increasing centralization of ballot counting has led to the use of computer systems whose integrity and reliability may be in question; typically these systems are based on proprietary software that has not been independently audited for accuracy. In addition—as recently happened in 2008 during the Democratic

primary election for county sheriff in Webb County, Texas—precinct counts may either be accidentally misplaced or maliciously discarded, leading to inaccurate vote tallies.¹

Consequently, assuring the public of the accuracy and reliability of such concealed counts rests upon the adequacy of post-election audits. We make the uncontroversial assumption that the overarching goal of a proper post-election audit² is to provide the public with verifiable assurance that election outcomes are correctly certified, and to do so in a timely manner.

Motivated by common concern for the integrity of elections, systematic monitoring and auditing of elections is recommended by political scientists, mathematicians, computer scientists, and election integrity advocates [33, 30, 18, 22, 15, 42].

Changes in voting system designs and the use of open standards for election data reporting would increase the convenience of methods for detecting and correcting vote miscount and reveal the causes of errors, thus contributing to overall improvement of elections systems [45, 13].

Various *ad hoc* groups of specialists and citizens regularly advocate for transparent audits, and recommend improvements to existing post-election audit approaches. [5, 29, 11, 10, 9, 12, 32]. In this paper we synthesize the lessons learned from recent experiences with electronic vote counting, and identify the additional elements necessary for an audit of election integrity. We hope to contribute to developing a set of standards by which citizens can be confident that their votes are being fairly and correctly counted.

Post-Election Audit Procedures

The effectiveness of post-election audits in detecting vote count errors depends on the precise procedures used to conduct the audits. [23, 24, 37], [34, p.33–39],[5, 31],[28, sec. 4.1]Consequently, the utility of each individual procedure as well as the collective operation of audit procedures as a whole is essential and integral to a post-election audit.

¹This article does not directly address the similar issues associated with the increasingly widespread use of electronic voting machines. These systems, adopted in response to the Florida recount debacle in 2000—which revealed the disadvantages of older, mechanical voting systems such as the Hollerith-inspired punched card ballots in widespread use in that state and others—and Congress’ passage of the Help America Vote Act of 2002, introduces a new vulnerability in the system by not keeping an independent record of votes cast besides the tally kept on the machine, which may be subject to miscounts due to accidental software flaws or deliberate miscounting by maliciously-programmed machines.

²As used in this paper, a “post-election audit” is a check of the accuracy and reliability of reported election results that is conducted by (1) manually counting voter-verified or voter-marked ballots associated with randomly sampled and reported vote counts, and (2) checking such additional records and processes as are necessary to evaluate and assure the integrity of the electoral process as a whole.

Flaws in post-election auditing procedures provide loopholes allowing accidental errors to be covered up or can be used by perpetrators to avoid detection of vote fraud. Our assessment is that all of today's state post-election audit procedures leave open avenues that allow vote count errors to escape detection.[3, 41]

The procedures described in this article are crucial for detecting any vote miscount, or addition, subtraction, substitution, or tampering with ballots that may affect election outcomes.

Definitions

“Audit unit” is defined in this article as a tally of votes that is publicly reported for an election contest. This tally is obtained from a group of one or more ballots that are either:

- counted at one place and time, or
- counted by one voting device, or
- cast by voters who live in the same voting precincts or districts.

Audit units can be precinct vote counts, electronic voting device counts, or batches or decks of paper ballots. Audit units can be counted by hand or by automatic tabulating equipment where each tally is associated with a number of ballots maintained as a group. An audit unit or auditable vote count may be an individual ballot only if the voting system produces a public report of vote counts on each ballot with humanly readable identifiers for individual ballots and yet preserves ballot privacy.

“Election outcomes” are the winners or losers of an election contest.

Before the Audit Begins

Limitations of post-election auditing

Post-election vote count audits as described in this article, are *not* designed to detect false voter-registrations, voter fraud, vote-buying, voter coercion, or all methods of ballot substitution or tampering by election insiders. Public control and oversight over all election processes including absentee ballot handling, pre-election audits of ballots and ballot definition files, and separate investigation techniques may be necessary to detect these types of problems.

Independent expert design and oversight

Audits defined and coordinated by the same organization whose work is being audited or investigated do not work. In any field, such self-audits often cover up or fail to report errors that are discovered during the audit process. The public should be permitted to review and comment on auditing procedures before they are implemented.

To provide the public with assurance that election results are accurate, audits should not be overseen by election officials, employees of voting machine vendors, or persons who make decisions on what voting systems to purchase, etc. The League of Women Voters and others have suggested creating an independent election audit oversight board in each state that includes mathematicians, computer scientists, gaming experts, political scientists, and open government advocates appointed in a nonpartisan and bipartisan manner [24, 41]. This independent election audit and recount board would:

- design and oversee the audit process,
- develop, evaluate, and update audit plans,
- provide for public review and comment,
- coordinate with election officials and vote count auditors,
- decide whether to expand the audit sample size or to certify an election contest,
- publish a report evaluating the efficacy and efficiency of the audits, and
- advise election officials and legislators of any problems or recommendations to improve voting and election systems, and
- help evaluate the auditability of new voting systems considered for purchase.

Only one state today, New Mexico, uses independent auditors to administer its post-election audits.

Reliable measures of voter-intent

There are at least four known ways of undetectably tampering with touch-screen digital recording electronic (DRE) voting machine-printed paper-roll ballot records to make them match altered vote counts and thus avoid error detection by post-election auditing. [35, 4] The National Institute for Standards and Technology Voting Project notes that “[i]t would

have to be clear... that the methods for voting systems to be auditable must be highly reliable and robust, and that today's DRE voting systems would not meet this requirement." Today, voter-marked paper ballots are the most reliable measure of voter intent for auditing.

Security of ballots and records

Election audits should review procedures for securing the election system (machines, ballots, servers, transportation, storage, ballot storage devices, pollbooks, etc.), as well as doing reconciliations and a statistically valid manual check of the vote count.

Independent security experts should design and evaluate chain-of-custody and security procedures for ballots and election audit records. These security procedures and processes should be open to public scrutiny, comment, and oversight.

Often election officials follow procedural recommendations of voting vendors who espouse the discredited principle of "security by obscurity" and keep chain-of-custody and security procedures secret from the public. Security by obscurity assumes that we do not have to secure ballots and election records from insiders, only from outsiders. Such practices still permit undetectable insider tampering and inspire little confidence in the integrity of the process.

On the other hand, good election security systems would partially rely upon public and bipartisan oversight and be designed with the help of some of the many available experts who design security systems for computers and financial institutions. Standards for moving and storing ballots and records should employ multiple persons watching the process with the idea that at least one of these people will be honest.

Keeping chain-of-custody records telling who accessed the records is necessary but not sufficient. If ballots or other audit records are added, subtracted, substituted, or tampered with, then audits will not effectively check the accuracy of reported election results.

Major differences exist between banking and voting that make elections much more difficult to secure than financial institutions. For example, banking requires customers to be clearly identified with their bank accounts, whereas elections requires that voters are never associated with their ballots due to the requirement for a secret ballot.

Committing the data first

The audit units that sum to the tally of the reported results must be publicly reported in an auditable vote count report that is made public prior to conducting the random selections of audit units. Otherwise, audit units not selected for auditing may be undetectably tampered

with to achieve a fraudulent outcome.

Therefore, a first step is to check to see that all audit unit tallies were included in and correctly summed by the central tabulator. Central tabulators have been a source of error in reported vote counts. Ideally each jurisdiction in a state report results in a common format that is both machine and human readable by a certain date and time as soon as possible after polls close.

Many states do not publicly report their audit units and fail to show that their audit units were used to tally the election results. For example Utah, Nevada, New Mexico, and Colorado randomly select “machines” or “ballots” that are not associated with any publicly reported vote count. Colorado does post-election machine testing by selecting up to 500 of its centrally counted voter-marked paper ballots per county and re-runs these ballots through an optical-scan machine after the election, comparing the new machine count with a new manual count. While such procedures may test the ability of the machines to count under limited, controlled circumstances, this procedure obviously does not detect errors in the reported election results. Many conditions are unique to counting the election results that will not be replicated in this secondary, later recount.

In addition to publicly reporting vote counts of audit units before selecting the units, polling place vote counts should be publicly reported at the polling places when polls close. This allows any votes that are lost or altered in transit from the polls to be detected. However, some states such as Utah and Hawaii fail to publicly post polling place vote totals at the polls when polls close, thus allowing ballots to be possibly lost, substituted or altered without detection during transport from the polls. Vote counts must be publicly committed as polls close and before ballots and records are transported from the polls in order to ensure that an audit can detect all types of outcome-altering manipulation.

To publicly commit the audit units, reports of all audit units used to tally the votes are required. Yet surprisingly today’s voting system tabulators are not designed to report auditable vote counts comprised of ballots that are routinely counted and stored together.

Uniformly sized audit units

Audits are more efficient—require auditing fewer ballots for the same confidence in election outcomes—if audit unit sizes are uniform; in other words, if reported vote counts are comprised of roughly the same number of cast ballots.

If a uniform random selection method is used—i.e. if each audit unit has an equal chance of being selected for auditing—then it is quite possible that audit units containing

a relatively large number of votes will not be selected for audit, even though it is possible (perhaps even more likely) that incorrect tallies will arise in larger audit units, and the larger units may collectively account for margin of victory in the contest [44, 43, 3]. Thus, if there is a large variation in audit unit size, a larger sample size—more audit units or more ballots—is needed to achieve a desired level of confidence in election outcome accuracy.

Planners should try to ensure that audit units will all be roughly the same size. However, unless individual ballots are the audit unit, some variation in audit unit size is inevitable because the number of voters voting at each precinct or polling location and who use each voting machine varies.

Subjecting all ballots to auditing

All early, provisional, polling place, and mail-in ballots should be included in the universe of ballots that might be potentially audited; otherwise, malicious actors may choose to manipulate ballot counts that they know *priori* will *not* be audited.

For example, Utah does not audit any absentee or provisional ballots and California does not audit absentee ballots that are counted after precincts are randomly selected for auditing.[16]

Ballots deemed to be ineligible should also be subjected to auditing to be sure that none of them were incorrectly deemed ineligible. If ineligible mail-in and provisional ballots are not audited, then it is possible for sufficient numbers of eligible ballots to be accidentally or maliciously rejected to cause an incorrect election outcome. Election officials must publicly report the number of ballots that were cast and not counted. Auditors should randomly check a sufficient number of mail-in and provisional ballot envelopes that election officials judged to be ineligible. The disposition of all mail-in and provisional ballots should be recorded as part of the audit.

Unused printed ballots likewise should be audited. If unused ballots are not audited, then printed ballots not used by voters could be filled out prior to or during an election and substituted in place of voters' ballots. In the case of ballot-on-demand printers, at a minimum the paper media for the ballots should be identifiable and subject to strict inventory control.

Again central tabulator design flaws make auditing of absentee and early voting ballots unnecessarily difficult and time consuming because they provide only precinct tallies and are not designed to provide tallies for individual DRE memory cards or for decks or batches of centrally-counted absentee and provisional ballots that are counted and stored together.

This is particularly troublesome with early voting where many precincts' ballots may be cast and counted by one DRE machine and for absentee mail-in ballots that are not counted and stored in precinct groupings.

Selecting Audit Units

Defining the audit unit

The audit units must be defined prior to the election. Are precinct vote counts, machine vote counts or the vote counts for batches or decks of optically scanned ballots going to be the audit unit? Because today's central tabulators are designed only to report precinct vote totals additional planning and work is required to use the tallies for batches of absentee ballots or for individual machine memory cards as audit units. Some of the procedures required to use audit units other than precincts are described later in this article.

Sizing the audit sample

When the goal of post-election auditing is to ensure the accuracy of election outcomes, sufficient audit units should be sampled to provide at least a 95% chance for detecting one or more miscounted audit units where the minimum number of miscounted vote counts could cause an incorrect election outcome.[21] An insufficient sample size, even if no discrepancies are found between manual audit counts and reported results, does not provide a statistically acceptable level of confidence that an election outcome is correct. It is unlikely that voters would be comfortable knowing that the audit only insures against an incorrect election outcome say, 25% of the time.

Confidence or risk-limiting audits conducted to provide statistical certainty in election outcomes require doing individual calculations on the detailed reported audit units in order to determine the minimum number of audit units that could be miscounted to cause an incorrect election outcome and then sizing the sample size to detect at least this amount of miscount. Unfortunately today's voting machines do not provide convenient usable reports or perform these calculations for us. Open source programs could take as input the list of audit unit tallies for each election contest and quickly do the audit sample size calculations, allowing the public to verify the accuracy of these calculations by using another open source version of the program. However, today's voting systems do not use open data formats so that independent local programmers can not conveniently write such programs.

Losing candidates select some audit units

Confidence or risk-limiting post-election audits premise sample size calculations on the assumption that audit units with suspicious-looking vote counts will be manually counted in addition to the randomly selected sample. Specifically, confidence election audit sample size is based on an assumption that any vote counts with more than an assumed rate of margin error, say 40% or 50%, would be immediately suspicious and be investigated without the necessity of being randomly selected for an audit [23, p. 14],[24],[39, p. 7],[1],[28, p. 70],[41].

Therefore candidates or their political parties can be asked to select one or two additional audit units. These additional selections must be audited in order for the audit to achieve its stated probability for detecting incorrect election outcomes. Otherwise a perpetrator could freely cause a higher rate of margin error in a small number of audit units to undermine the effectiveness of the audit sample size and avoid detection by audit.

Auditing each election jurisdiction

Innocent ballot programming errors, voting system problems, or fraud that is peculiar to one jurisdiction could be missed unless at least one audit unit is selected from every separately-administered jurisdiction where a contest occurs.

These additional selections must be made after the initial random selections because if made first, high-population areas would be insufficiently sampled, enabling a perpetrator to increase the chance for escaping detection of vote fraud by targeting larger cities.³ (XXX cite Lehto, private communication with the authors, rather than a footnote here—it seems out of place?)

Timing of the sample

Timing of the selection of audit units is crucial. Some states randomly select audit units for auditing prior to completion of the counting and reporting of the votes, thus enabling votes to be freely misreported for all audit units that were not selected for auditing. For example, Utah randomly selects “DRE machines” to be audited on Election Day before polls close and before election results are tallied or publicly reported, so that any vote count not selected for auditing could be deliberately misreported. [19] California selects precincts for auditing prior to counting the absentee and provisional ballots, yet uses those

³Thank you to Paul Lehto for pointing this general issue out in 2006 on a National Election Data Archive email discussion list.

same precincts to audit absentee and provisional ballots. These practices provide a road map for which as-yet uncounted ballots may be misreported with impunity.

Probability sampling methods

Even small variations in the details of sampling methods can result in biased samples that could miss detecting vote count errors. Simple random samples or stratified random samples should be used when selecting audit units. Fair and efficient methods for randomly selecting vote counts for auditing have been developed by computer scientists and mathematicians such as ten-sided dice or open-source pseudo-random number generators [14, 7, 2, 27, 36].

Failing to use probability sampling methods could result in deliberately avoiding inaccurate vote counts. For instance following the Ohio 2004 election, election officials in Cuyahoga County were discovered to have deliberately pre-selected audit units that they knew would match the reported machine counts in order to avoid expanded audits.⁴

During the Post-Election Audit

Reconciling voters and ballots

A reconciliation of voters and ballots for the entire jurisdiction is necessary to detect cases when votes or ballots are missing from the initial reported auditable report. Therefore the initial step in a manual vote count audit is to reconcile the number of voters processed with the number of ballots printed, cast, counted, spoiled, unused and judged to be ineligible for the entire election jurisdiction. Also, the number of absentee and provisional ballot applications and ballot envelopes received must be reconciled with the number that are counted or rejected as ineligible.

Election administration is handled by jurisdictions such as counties, townships, or parishes. Many U.S. jurisdictions only reconcile ballots and voters at the polling locations but fail to reconcile ballots and voters jurisdiction-wide. For example, Utah election statute requires the destruction of unused paper ballots when polls close, prohibiting county-wide reconciliation and requiring the destruction of evidence that would reveal cases when ballots were substituted for voters' legitimate ballots. Currently Utah does not publicly release even its polling location reconciliations.

Without comprehensive jurisdiction-wide reconciliations of ballots and voters after an election, then sufficient ballots to change an election outcome could be subtracted, added, or

⁴See "After Ohio's recount rigging convictions in Cuyahoga, is Coshocton County next?" by Bob Fittrakis and Harvey Wasserman, Mar 2007 <http://www.freepress.org/departments/display/19/2007/2462>

substituted without detection. Performing jurisdiction-wide ballot reconciliations ensures that the number of ballots printed equals the number of cast ballots, plus the number of spoiled ballots, the number of unused ballots, and the number of ineligible ballots.

Audit immediately after selecting units

Access to ballots and audit records must be prohibited between the time that the audit units are selected for auditing and when the audit is begun. If audits are not begun immediately after the random selections, selected ballot and audit records can be manipulated to match erroneous reported results. Immediately following the random selections of audit units the ballots and audit records should be brought to the auditors to begin the reconciliations and manual counts.

Election officials have been observed going through ballots after it was determined which ballots would be audited and before the audit. In Arizona, seals on ballot bags were found to be compromised before the post-election audits. (XXX cite needed?)

Public participation

The public must be able to fully participate. The public should be allowed to observe close up all security procedures, audit procedures, random selections, manual counts, including being allowed to object when they believe that a procedure is being improperly followed or a vote has been misinterpreted, miscounted or mismarked during the manual counting. The public should have access to audit records and reports including all auditing tally sheets, all reconciliations, and audit results. [16, 17] Otherwise a group of auditors could subvert the effectiveness of the audits.

For decades elections have not been subjected to independent scrutiny. Many election officials and voting machine vendors appear to believe in the discredited principle of “security by obscurity” in which all security procedures are kept secret except from vendors, technicians, and election administrators.

Audit records availability

Auditors must have timely access to election records to detect cases of ballot substitution, addition, and subtraction, and to try to determine the cause of any vote miscount that is detected during an audit.

Election audit records that must be available to auditors include voting machine testing plans and results, electronic voting device and automatic tabulating equipment audit

and system log files, ballot definition files, voter-verifiable paper records and paper ballots, provisional and absentee ballot envelopes and applications, ineligible and unused and spoiled ballots, digital storage devices that store ballot information and/or voting results information stored in a non-volatile form, records of purchased material and services including purchase orders and inspection records on purchased parts and services, voting system redundant vote data, election data media devices, polling place event logs, precinct tally results, central count tally results, consolidated results, records created at the polling places or county election office, written procedures provided to poll workers and election judges, poll books and voter registration materials, written chain of custody and security procedures for regulating access to paper and electronic ballot records, and for regulating access to electronic voting devices and automatic tabulating equipment, chain of custody logs containing signatures documenting access and the reasons for it, logs of security seals and access to election-related storage areas, video records of surveillance cameras.

In some states such as Utah, open records laws do not apply to any election records and election officials do not allow public access to any election records that are necessary for verifying the integrity of the electoral process and the audits themselves. [19]

Random assignment of auditors

Random assignment of counters to count specific vote counts helps to ensure that persons with opposing political views are on the same team that manually determines and records votes during the audit. Use well-tested manual counting methods that have been developed [17] to ensure that auditors do not themselves miscount votes.

Voter intent standard

Instructions to auditors should ask auditors who manually count ballots to simply try to determine what the intent of the voter was, and to observe and record, for each audit unit, whenever voters did not follow the instructions for marking voter-marked paper ballots.⁵ This approach is easiest for auditors and consistent with the overarching goal of determining if an election outcome correctly reflects what voters wanted.

A “determine-what-the-machine-should-have-done” approach makes the job difficult for auditors who do not have engineering training and do not know how the machines were

⁵Heleni Thayer, in a 2008 correspondence on a National Election Data Archive email discussion list, suggested asking auditors to record it whenever they notice that a voter failed to follow ballot-marking instructions. Recording occasions when voters fail to follow marking instructions would make it easy to determine the proportion of discrepancies that can be explained by voter errors, or if the causes of discrepancies require further investigation.

programmed to operate. Such a “determine-how-the-machine-should-have-interpreted-the-ballot” approach results in inconsistent reporting of the discrepancies and may neglect to report discrepancies that are caused by voter errors. Connecticut requires manual counters to try to determine whether or not the machine should have been able to count the vote.⁶ Colorado auditing rules also require voter intent to be judged more like the machine would respond, requiring consistency by the voters to justify counting erratic marks.

Regardless of whether discrepancies are caused by machines or by voters, the audit must report the manual counts judging who voters intended to elect.

Effective, efficient counting methods

The manual counting method determines the number of counters on each team that is necessary for the manual tallies to be most accurate and efficient. The manual counts of voter-verified paper ballots will be more accurate and speedy when the team doing the hand counts has the proper number of team members for the counting method - the read-and-tally or the sort-and-stack method. [17]

Research shows that optical scan paper ballots facilitate more accurate and faster counts than paper-roll ballot records or video verification systems. [28, 25] Some counting methods perform with the same amount of error on sequential instances of counting. Other methods such as “sort and stack” are designed to converge on a result after repeated counts.

After the Manual Counts

Discrepancies

When discrepancies are found between the manual and reported audit units, the hand count should be performed again independently to check its validity, or in the case of “sort and stack,” a further check of sort and a further count of the stacks should be done.

Opportunistic recounting should not be done with awareness of the “desired” result. Otherwise it is possible to reconcile opportunistically by another mistake.

If the discrepancy between the initial versus the manual audit tallies is not found to be due to a hand count error, then an attempt should be made to investigate the cause of error. The record or records (or missing records) responsible for the discrepancy can often

⁶See Substitute Senate Bill No. 1311 Public Act No. 07-194 AN ACT CONCERNING THE INTEGRITY AND SECURITY OF THE VOTING PROCESS. <http://www.cga.ct.gov/2007/ACT/Pa/pdf/2007PA-00194-R00SB-01311-PA.pdf>

be located by using precinct specific or batch specific information to reduce the number of ballots containing the discrepancy.

Manual tally as official record

Unless there is evidence of tampering with the paper ballots, the secured voter-verified paper ballots should always be considered the correct record of the voters' votes and the manual tally of such paper ballots must be considered the correct record of the vote.

Missing/damaged ballots are discrepant

Assume that missing or unreadable paper ballot records are discrepant with the reported vote counts in a way that favors the reported winner's margin over the closest runner-up.

When missing or illegible paper ballot records are assumed to match reported election results by excluding any audit units having such missing or illegible paper ballots from auditing, then votes can be undetectably miscounted as long as the machine that miscounted them is made to fail in some way before poll closing or as long as the paper ballot records are lost or damaged. It is common practice today to exclude from an election audit any vote counts created by machines that experienced a failure or that have missing or damaged paper ballot records and to assume, without evidence, that any such missing or damaged ballots match the reported results. Such a policy provides a road map to perpetrators for how to successfully commit vote fraud.

When deciding to expand the audit or to certify an election outcome, missing or damaged records may necessitate expanding the sample size. If sufficient voter-verified ballots are missing or damaged to put the outcome in question, then an election outcome may not be able to be determined on the basis of the voter-verified paper ballots by a manual audit and a top-two runoff election may have to be held in order to determine the legitimate winner.

Reporting the discrepancies

Misreporting election audit discrepancies could result in certifying incorrect election outcomes. Discrepancies found during an audit and the causes of such discrepancies when known, should be reported at least 24 hours in advance of certification of the election outcome.

To certify or to expand?

The general rule is that the auditors should analyze the discrepancies and expand the audit sample size if the accuracy of the reported initial election outcome is in question, or otherwise certify the election outcome.

If the sample size and the analysis of the discrepancies found during an audit are not adequate then an election audit does not provide assurance that the election outcomes are correctly reported. Incorrectly analyzing election audit discrepancies could result in certifying incorrect election outcomes.

A commonly used approach today is to certify an election outcome whenever there is less than an arbitrary fixed amount or fixed rate of discrepancy and to otherwise increase the audit sample size [39, 40, 38]. For instance Minnesota requires that if there is a discrepancy greater than one-half of one percent, then the sample size must be increased by at least three precincts in the same jurisdiction where the discrepancy was discovered.⁷ Other commonly used approaches are to audit additional precincts at the discretion of the elections official or to expand an audit if any discrepancies are found in the manual audits. These methods could result in unnecessarily expanding audit sample sizes in wide margin contests and some of these methods could possibly result in certifying incorrect outcomes in very close contests.

If the audit sample size is not sufficient, then an election outcome will still be doubtful regardless of small or zero discrepancies. Decision algorithms for determining whether to certify election outcomes or to expand the manual audit sample size need further research and development [20, Appendix E]. Methods for analyzing discrepancies will be found in a subsequent article by this author.

Completing audits prior to certification

Post-election audits must be completed and audit records and results must be publicly posted prior to certifying election contests.

Post-election audits that are conducted after election results are certified and the election contest period has ended, do not provide for accurate election outcomes. Florida conducts post-election audits only after the election results are certified.

Audit results need to be posted to the public so that independent evaluations of the quality of the election can be made. These reports will preferably convey an understanding

⁷See <https://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H3833.2.html&session=1s84>

of how the audit was performed as well as details of audit results and any adjustments to correct the reported election results that the audit necessitated.

Impediments to Auditing

Commercial voting systems are not designed to provide convenient methods for detecting and correcting vote miscount. Additionally, with the current designs, even if miscount is detected, it is not possible to know how, when or where the errors occurred or who caused them. Given the substantial obstacles to performing convenient post-election audits, it is not surprising that many States' existing election "audit" procedures fail to actually check the accuracy of their publicly reported election results.

Tabulators produce unusable data

It can require many hours of tedious detail work to reorganize the data produced by today's voting system reports into a usable form.

The data produced by tabulator reports may be in PDF format and require re-entry to use for auditing calculations. Data reported in XML or in spreadsheet format may be in a form that is not numerical, not editable, is missing crucial data, or may fail to be organized into logical columns or units that can be used by other programs.

Proprietary data formats

Proprietary data formats used by voting vendors make it difficult to share data or to interchange voting system components, increasing costs and reducing functionality. Voting vendors' use of proprietary data formats and their lack of willingness to publicly release information about their data formats, makes it difficult for local programmers to generate auditable reports that are necessary for efficient post-election auditing.

Tabulators do not report vote counts for ballots that are stored together

Voting system tabulators typically aggregate and report vote counts by precinct and, if set correctly by election officials, will also report whether the votes were cast in the polls on Election Day, during early voting, or by absentee ballot. To do this, election officials must

configure individual memory cards to be used for precinct, early voting, or absentee voting. Voting tabulators do not report the voting machine or the batch of ballots for the counted votes.

In other words, today's commercial voting systems do report counts by precinct but do not report tallies for the ballots that are recorded and stored on each memory card nor do they report the tallies for batches or decks of ballots that are counted at one time on central count optical scanners and stored together.

On the other hand, election officials naturally group ballots together that correspond to votes recorded on one memory card (a portable electronic ballot box) used in a DRE touch-screen machine or used in a polling location optical scanner or used to store the counts of paper ballots counted by a central count optical scanner. Often the contents of the memory card match a physical group of paper ballot records.

To compound the problem, precinct-based optical scanners and DRE touch-screen machines often count ballots for multiple precincts, whereas the central tabulators and equipment used for tabulating early voting do not report any vote counts by the machine. Thus, if one is using the tabulator reports to select audit units, it is necessary to select and manually count precincts, even though ballots are not sorted or stored by precinct. Central count optical scan paper ballots are normally counted and stored in batches or decks containing multiple precincts' ballots, but the tabulator only reports the accumulated total for all batches of absentee ballots counted altogether broken out by precinct, although hundreds of thousands ballots may have been counted from numerous precincts.

False reports by tabulators

Sometimes central tabulators fail to upload and tally the votes of entire memory cards (Ohio cases; Humbolt County, Calif. 2008), but nonetheless report that these votes were successfully uploaded. Conversely a central tabulator may report that the memory card's vote counts have not been uploaded when they were, causing an election official to try to upload these counts again, perhaps counting these votes more than once.

The Premier, formerly called Diebold, central tabulators some times drop the counts for the entire first batch of paper ballots counted by the central count optical scanner, causing hundreds of votes not to be included in the reported election results.⁸

Central count optical scanners often miscount the number of total ballots cast, partic-

⁸“Serious Error in Diebold Voting Software Caused Lost Ballots in California County Update” By Kim Zetter, December 8, 2008 <http://www.wired.com/threatlevel/2008/12/unique-election/>

ularly when ballots have two pages that are separated or when the scanner’s ballot feeder malfunctions and grabs two ballot sheets at one time. Central count optical scanners may provide no way of tracking whether or not a batch has been run already or of reporting the number of batches that were counted. Consequently, some batches may be run twice by mistake or not run at all by election officials.

Tabulator reports that fail to include entire vote counts counted by a DRE machine or entire batches of ballots in the tallies are particularly troublesome for audits because the selection of audit units is done by using the tabulator reports that allegedly include “all” auditable vote counts. A total county-wide reconciliation of the number of voters with ballots cast is crucial to detecting these types of errors, but when discrepancies are found, they may be difficult to track down.

Paper-roll ballot records

Voter-verifiable paper roll ballot records used by touch-screen electronic voting machines (DREs) do not provide a reliable measure of voter intent because they can be undetectably manipulated to match fraudulent electronic votes no matter how diligent voters or election officials are [4]. In addition, voters with disabilities may find it difficult, if not impossible, to verify the accuracy of such paper-roll ballot records.

In addition, DRE paper roll voter-verifiable paper trails (VVPTs) are time-consuming and error-prone to manually count [25].

- When a voter rejects a paper roll ballot, the “Rejected Ballot” stamp appears after the printed ballot, so that the counting team must unroll and re-roll the ballot rolls to either see if the ballot was rejected before beginning to count it, or recounting and subtracting all the votes from the recorded manual tallies whenever a “Rejected ballot” stamp is discovered.
- VVPTs are easily damaged because their printers are often inexpensive and not well-designed, and paper rolls may be loaded incorrectly causing them not to print or to jam and print over other ballot records.
- DRE touchscreens are often used to cast and count more than one precincts’ votes, yet VVPTs are not sort-able by precinct, making manually counting a selected precincts’ ballots difficult.

- Some paper roll ballot records are designed to print numbers without any identifying text for ballot issues and for judges, making it difficult for voters to verify their ballot choices and difficult for auditors to manually count the votes.

Political obstacles

Canvass periods in many states are too short to complete the audit prior to certifying election outcomes. Canvass periods should be extended to 28 days.

There is political opposition to auditing among election officials and voting vendors. Groups such as The Election Center and The Election Technology Council have in the past formally opposed federal requirements for auditable voting systems and for post-election audits. Similarly some election officials have urged State legislators to oppose bills requiring auditable voting systems or post-election audits. Election officials often conduct “audits” in ways that would not detect vote miscount or determine if the voters’ choices are the certified result. It may be human nature to avoid exposing, or to overlook, the mistakes, errors, or problems that occur in one’s own work.

Obstacles to Accountability

“Accountability” is the capacity, when errors occur, to learn how, when, and what caused errors, and who was responsible for causing the errors. Today, most commercial voting systems lack accountability.

Incomplete, erasable log files

Technology to create unalterable write-once-only log files has been available for decades, but was not employed in today’s voting machines. Voting system activity logs may be altered or changed after they are created and fail to log all events that occur.

Problems related to voting system logs were described in the California Secretary of State Debra Bowen’s “report to the election assistance commission concerning errors and deficiencies in Diebold/Premier gems version 1.18.19”. [8] Bowen reports that the tabulator

“... fails to record in any log important system events such as the deletion of decks of optical scan ballots after they have been scanned and entered into the GEMS election results database. Second, it records the wrong entry date and

time for certain decks of ballots. Third, it permits deletion of certain audit logs that contain-or should contain-records that would be essential to reconstruct operator actions during the vote tallying process.”

In violation of federal certification requirements, an early version of Diebold/Premier tabulators have “Clear” buttons that allow election officials to easily delete computer log records, and methods exist that allow alteration of log files and changing vote counts without creating log file entries.

Log files should be a permanent unaltered complete record of all activity and access that occurs on a voting system. Without unalterable activity files, it is more difficult to detect illicit activity. the need is for activity logs to be independently recorded in such a way that undetected tampering is extremely difficult. Voting system audit log deficiencies in combination with insufficient password protection make it impossible to monitor operator access to the tabulators.

An alternative approach is the one described in “Trusted Logic Voting (TLV) approach”⁹. Here a monitoring and control program runs at the level of the operating system (akin to today’s antivirus systems approach). Such root level control programs are at the heart of how computers function. Program execution is tracked and any operations or patterns that deviate from the recorded and previously verified activity are immediately blocked in real time during voting, and the machine deactivated and balloting stopped. Similarly in post election, these monitoring programs can prevent access to the computer completely. Essentially preventing anyone from activating the computer once balloting is ended for an election. Then the only way into the records for unauthorized access is to physically remove the storage device(s) from the ballot computer and place it in another computer. Such tampering would be detected by physical seals on the equipment.

Backdoors

The use of backdoors in election computer systems has to be eradicated and outlawed. Backdoors exist because of poor development processes and weak testing and verification procedures along with the absence of secure setup and configuration procedures with oversight.

Backdoors are designed to allow insider staff to reset equipment back to some initial state as a convenience to those staff, saving vendors time and money. This also applies to last

⁹<http://www.trustedelections.org/>

minute changes to software particularly under the guise of bug fixing. For example Diebold staff performed unsupervised and unverified emergency updates to their DRE systems in the 2007 elections in Maryland two weeks before the actual balloting occurred. Again secure update procedures are called for as part of Trusted Logic Voting with the aim to ensure that the only way for unauthorized access to occur is by physically removing storage devices from a computer chassis into another open computer system, apply changes, then physically re-install that tampered storage device back into the original computer chassis. With modern computers, it is entirely possible to define totally secure update procedures and authentication techniques along with rolling random entry key techniques so that not even the original software creators can access their own systems once authority and control of the software has been turned over to the proper election authorities. Such procedures should be mandated as a matter of course for election systems.

Weak password protection

Some of today's voting systems use the same password for all users, so when there are multiple election staffers using a voting system it is not possible to tell who did what. Again there should be absolutely no possible access to the underlying operating system on voting machines via normal login accounts. The only action should be for voting officials to initiate voting or vote counting on the machine, and then at the end of balloting to shutdown the system and prepare the totals. Any other action and accounts should be outlawed. Then the only way to change anything on the computer must be a one-time secure authenticated process completely controlled by election authorities and performed as part of formal preparation of voting systems for an election and including loading of the ballot details, software corrections and resetting that can be overseen by candidates or their appointed representatives as well.

Insufficient tabulator reporting

Again, the failure of central tabulators to report which machines were used to create each vote count included in the tally, or to report individual machine tallies, makes errors difficult to trace back to individual DRE machines. Reports generated by the central tabulator report only one cumulative total for centrally counted optical scan ballots, rather than the tallies for each separate batch of optical scan paper ballots, making errors difficult to check or trace back to specific batches.

Use of digital signatures

Today's commercial voting machines use digital signatures as a means to cloak weak procedures and as a crutch so that vendors may claim that their systems are tamper proof. As with any lock and key system, with the digital signatures being the key, the security is only as good as access controls to the digital signatures themselves. In most current cases the vendors control and have access to these on behalf of their customers. Therefore in the future digital signature control has to be with election officials and completely separated from vendor staff. Then voting systems must use digital signatures to both identify the source of voting artifacts (as incorporated into OASIS EML voting records) but also to dramatically reduce the chance that subsequent tampering may occur manually.

Political obstacles to accountability

Some states do not allow public access to voting system log files or other crucial election records. Thus illicit activity or alteration of vote counts can not be detected by reviewing these records and voting system activity logs.

Instead the reverse should be the norm. The computer records used during the election process should be freely and publically accessible after the election as a complete record of what occurred. The OASIS EML open data standard provides the means for such end-to-end traceability of counting and for independent auditing and confirmation of election results by any outside party having software that supports the EML standards.

The State of California has taken an important step in this direction by providing media sources with real time precinct level results during elections starting in 2007¹⁰.

Ways to work around the impediments

Practical workarounds have been devised for overcoming some of the obstacles to conducting post-election audits.

Some computer programmers, working with local election officials, have devised methods to generate auditable reports of vote counts for ballots that are grouped in a batch and stored together and marked to reflect the source of the audit units that are used to tally the reported results.

¹⁰http://www.sos.ca.gov/elections/ca_elect_results/result_example.htm

Eliminate or reduce DRE machine use

To ensure that a valid record of voter intent is used for manual audits, reduce or eliminate the use of DRE touch-screen voting machines that cannot be guaranteed to produce a reliable record of voter intent.[4] The California Secretary of State, Debra Bowen, has reduced DRE touch-screens to one per precinct. The Maryland and Tennessee legislatures have voted to stop using DRE voting machines and use voter-marked paper ballots. Florida and New Mexico's Governors successfully pushed for the elimination of DRE machines except for use by voters with disabilities. Numerous other jurisdictions are eliminating or reducing the use of DRE touchscreen voting.

Precinct audits of DRE machines

Providing at least one separate DRE machine for each separate precinct within the same polling location and training poll workers to ensure that voters know which digital recording electronic (DRE) machine to use will make auditing DRE paper roll ballot records much easier to do because all of the ballots cast on one DRE paper roll will be for the same precinct. California Secretary of State Debra Bowen wisely requires that each DRE voting machine only be programmed to count one precinct.

Sort paper ballots by precinct

So that the ballots can be manually counted and compared with the precinct reports that the central tabulators produce, paper opti-scan ballots should be sorted into precincts for manually counting in an audit. The California Secretary of State Bowen and other jurisdictions require sorting centrally counted ballots into precincts. In this case, a separate sample size must be calculated and drawn from any late-counted optical scan ballots that are counted after the initial selections of audit units.

Polling location as audit unit

To avoid the problem of having to sort the optical scan ballots into precincts and also to avoid the problem that DRE paper roll ballot records and DRE and precinct-based optical scan memory cards may contain votes for several precincts, the precinct reports for each polling location can be summed to report polling location vote counts [6, 32]. However

the large size of audit units requires manually counting more ballots to achieve an equal probability for detecting incorrect election outcomes. Therefore this method is less efficient.

Central-counted batches as audit unit

To create an auditable report of vote counts corresponding to batches of centrally-counted optical scan paper ballots, print and save to disk a summary report on the central tabulator after each batch of ballots is counted and then subtract the prior summary report from the current summary report in order to obtain the individual tallies for each additional batch of ballots.

This subtraction approach requires concentration, patience, and attention to detailed steps at a time when press and candidates may be pressuring election officials to report the results. Officials should be sure to save a copy of each report electronically in XML or in spreadsheet format under a unique descriptive file name. Officials should also print and save to disk a PDF copy of each cumulative report, clearly marking the printed copy with the information about which batch from which voting machine was uploaded right before the report was printed. Each time a report is missed, the audit unit size increases, requiring extra hand counting to achieve the same probability for detecting incorrectly reported outcomes.

Use a memory card for each batch of ballots

To make it easier to audit ballots that are centrally counted such as absentee and provisional ballots and precinct-voted paper ballots that are centrally counted, use a new memory card for each batch of ballots counted using the central count optical scanner. This preserves both a portable electronic ballot box (memory card) and its corresponding paper ballot records in an efficiently-sized audit unit.

In other words, a cumulative report is printed, hand-marked and saved to disk in two different file formats for every memory card (portable ballot box) whose votes are uploaded to the central tabulator.

Swap memory cards for early voting

Memory cards and paper rolls can be changed daily on any DRE touch-screens that are used for early voting, carefully labeling and securing the used memory cards and paper rolls

for later counting and auditing. Jurisdictions usually configure early voting DREs to count all precincts' ballots in the jurisdiction.

If the tabulator only reports precinct vote counts and the audit unit is precincts then an individual central tabulator report from each memory card is needed to reveal which early voting paper roll VVPTs must be unrolled and re-rolled to manually count the votes cast in the audited precincts. Swapping the memory cards also enables more efficient (smaller) individual memory card counts to be used as audit units. (See the following sections.)

If the memory cards are not swapped regularly on DREs used for early voting, then those early voting machine counts will be very large, making the audits either inefficient or ineffective unless all the early voting machines are audited.

The difficulty of obtaining auditable reports to efficiently audit DRE machines is one reason why the California Secretary of State simply requires 100% manual audits of all DRE paper roll VVPTs and requires that DRE machines are configured to count only one precinct each.

If election officials use this approach, of using new DRE memory cards daily during early voting, they need to keep in mind that it introduces additional security and recording issues that must be handled.

DRE machines as audit unit

If the audit unit is a DRE machine with paper rolls but the central tabulator does not produce a report of DRE machine counts, then officials can use a subtraction method to generate an auditable report of DRE machine counts for all election contests. In other words, officials can print and save a cumulative report generated by the central tabulator after uploading each DRE memory card and then subtract the prior cumulative reports' numbers from each subsequent cumulative report.

It should be noted that some voting systems do not permit this approach. The Hart Intercivic voting system networks all DRE touch-screen voting machines in the polling location, supplying only one "JBC" memory card or portable ballot box, for all the DRE touch-screen voting machines linked or "chained" to that JBC. This makes it impossible to obtain individual DRE machine vote counts by using the cumulative report subtraction method, making it a less efficient voting system to audit. It is possible to use the treat the entire chain of DREs connected to a JBC as one audit unit.

Write a program to subtract data

Hire a programmer to write an open source computer program to parse through the poorly formatted XML and other cumulative precinct reports generated by central tabulators and perform the subtractions to create an auditable report of vote counts for memory cards or batches of ballots. With a parsing program post-election audits can avoid many laborious hours of manual re-inputting of data from the summary reports into a spreadsheet so that the subtractions of the cumulative reports can be done for each election contest. [32] The same program can also be used to calculate audit sample sizes that would detect incorrect election outcomes.

Such programming efforts would be easier to accomplish if vendors would publicly release their data formats, or if vendors would instead use open data formats such as the Election Markup Language (EML) developed by OASIS (Organization for the Advancement of Structured Information Standards), a not-for-profit consortium.

Audit individual ballots

Auditing individual ballots is more efficient because it achieves a higher chance for detecting incorrect outcomes when the same number of ballots are manually counted, and it eliminates some of the complexities of calculating sample sizes and some of the complexities of audit discrepancy analysis.

Some voting systems include software that allows a laptop to be connected one at a time to each DRE touch-screen machine to download the individual cast vote records from each DRE machine [6]. If this feature is provided then one may download a copy of the cast vote records listing the votes on each ballot along with a human readable identifier that is also printed on each paper roll ballot record. In some voting systems, these electronic cast vote records are listed in the same order as ballots are cast on each DRE machine and the same humanly readable identifier is printed at the beginning of each paper roll ballot record.

Using the cast vote records, the votes can be transferred to a spreadsheet and summed for each individual DRE machine and if possible checked against the aggregated central tabulator totals by precinct. Then using the identifiers, a random sample of DRE paper roll ballots can be selected for manual auditing and the selected paper roll ballots' votes checked with the corresponding cast vote records.

Concerns with individual ballots as audit units include a lack of availability in most voting systems of cast vote records for the optically scanned paper ballots, the need to

publicly publish all the cast vote records to make the audit publicly verifiable, possible vote buying if voters could record their own ballot ID numbers, the necessity to sometimes merge small precincts before publicly posting cast vote records in order to protect voter anonymity, and when poll books that record voters in the order in which they sign in to vote are used it would be possible for someone to pair ballot records with voters, violating ballot privacy. Another concern is the ability to identify a voter by ballot style when special districts cause unique ballot styles to be associated with very few voters in coordinated elections¹¹.

Open data standards for voting data

Using open standards for recording and managing the election is crucial. This then transforms the situation from one of proprietary systems to open ones. Then independent reviews can more easily verify counts and totals, and independent test suites can be applied to ensure tabulation systems perform correctly during certification. Similar validation software can check to ensure that voting records do not contain erroneous or malicious information. It is important to make sure records contain only correct information and nothing else that may be used to corrupt a result.

The banking and health care industries, among others, have already implemented open standards for formatting and transferring electronic information data. Election officials should require standard open data formats for all future voting systems in order to improve interoperability and auditability. Existing obstacles to election data sharing could be overcome if forced by the Federal government. For instance, Congress passed the Health Insurance Portability Act so that people could take health insurance anywhere and that took two years to comply with the ISA standard. Likewise Congress needs to pass sweeping reforms to ensure that voting systems are built to be open, accessible, and auditable.

Accountable, auditable voting systems

Most of the obstacles to auditability and accountability presented by today's voting system designs can be eliminated by requiring the development of another generation of better-designed voting machines and central tabulators. The quickest, most economical solution may be to hire competent local programmers to create economical open source optical scan voting systems that use open data standards end-to-end and can use off-the-shelf

¹¹Coordinated elections occur when special district elections are administered by county election officials during regular elections, causing the number of different ballot styles to be very large.

computer system components. This would also require that States fund federal testing and certification as New York have looked at doing already to defray that otherwise substantial cost.

Election officials should carefully think through the system requirements needed to conduct an efficient audit for every election before specifying requirements for voting system and before negotiating contracts with voting machine vendors [26]. Independent experts who can provide objective input should also be consulted. It should be a prerequisite that election results should be open and public as California have demonstrated.

Conclusion

Post-election audit procedures designed to assure the accuracy of election outcomes are made indispensably necessary by modern computerized voting systems in order to uphold the checks and balances that are integral to our system of self-government. Given that the necessary post-election audit procedures defined above are followed, the post-election audit sample size must be sufficient to provide a minimum probability of at least 95% that any initial incorrect election outcome will be corrected prior to certifying the election contest. Achieving this goal requires changes in election data reporting practices as well as changes in post-election auditing practices that will vary from state to state and from voting system to voting system.

The obstacles to effective post-election audits that are identified in this paper are collectively both pervasive as well as deeply troubling, and their correction will involve difficulties, costs, and efforts by citizens, election officials, voting system vendors, and legislators alike.

To provide public assurance that any initial incorrect election outcomes are detected and corrected by post-election audits, the audits must:

- publicly publish all vote counts (audit units) used to tally the votes prior to when audit units are selected for auditing
- be independently overseen - not by election administration officials, nor by any voting system component vendor staffers or consultants
- use reliable evidence of voter intent such as voter-marked paper ballots
- evaluate the effectiveness of security procedures used to protect the integrity of ballots and other election records

- subject all ballots and all election jurisdictions to auditing
- use probability sampling methods to select audit units
- allow losing candidates to select additional audit units that look suspicious to them for auditing
- sample sufficiently to detect well-hidden vote fraud that could alter an election outcome
- reconcile all voters and ballots throughout the entire jurisdiction
- invite and include public participation in all aspects of auditing
- make all election records that are necessary to evaluate the integrity of the electoral process available
- accurately report and analyze any discrepancies found between the initial reported audit units and the manual counts of audit units, including discrepancies caused by voter error and by missing or damaged voter-verifiable paper ballots
- expand the audit sample size whenever the discrepancy analysis is consistent with an initial incorrect outcome
- never certify an election outcome until after completing the audit

Today’s voting systems exhibit cavalier disregard for the need to provide real auditing of their results. The obstacles to conducting audits are pervasive and deeply troubling, and can only be overcome with great difficulty, cost, and large effort.

In a speech to Congress in 1890, President Benjamin Harrison emphasized both the importance of heeding, and the penalties of not heeding, calls for election reform:

“If any intelligent and loyal company of American citizens were required to catalogue the essential human conditions of national life, I do not doubt that with absolute unanimity they would begin with free and honest elections. And it is gratifying to know that generally there is a growing and nonpartisan demand for better election laws; but against this sign of hope and progress must be set the depressing and undeniable fact that election laws and methods are sometimes cunningly contrived to secure minority control, while violence completes the shortcomings of fraud.”

Given this combination of importance, risks and rewards, few indeed will dispute the need to make real the promises of democracy by leaving an inheritance of self-government for future generations that is better than the one we were given.

Acknowledgements

Thank you to Alice Steiner, Co-President of the League of Women Voters of Utah and to Harvie Branscomb for reviewing this paper and making helpful style and content edits. Thank you to David Webber for many helpful content suggestions, including helping to rewrite the “Backdoors”, “Weak password protection”, “Use of digital signatures”, “Political obstacles to accountability”, and “Accountable, auditable voting systems” sections using his expertise in computer science and voting systems. Thank you to Paul Lehto for making constructive suggestions for the abstract, introduction, and conclusion. Also, thank you to the many persons who helped by reviewing my prior legislative post-election auditing proposals [24] or who informed me about their own experiences.

©2009 Kathy Dopp

References

- [1] Andrew W. Appel. Effective audit policy for voter-verified paper ballots in New Jersey. Princeton Computer Science Department Web site, March 1997. <http://www.cs.princeton.edu/~appel/papers/appel-nj-audits.pdf>.
- [2] Javed A. Aslam, Raluca A. Popa, and Ronald L. Rivest. On auditing elections when precincts have different sizes. Massachusetts Institute of Technology Web site, January 2008. <http://people.csail.mit.edu/rivest/AslamPopaRivest-OnAuditingElectionsWhenPrecinctsHaveDifferentSizes.pdf>.
- [3] Lonna Rae Atkeson, R. Michael Alvarez, and Thad E. Hall. The New Mexico 2006 Post Election Audit Report. Pew Center on the States Web site, September 2008. http://www.pewcenteronthestates.org/uploadedFiles/NM_Audit_Report1.pdf.
- [4] D. Balzarotti, G. Banks, M. Cova, V. Felmetzger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna. Are your votes really counted? testing the security of real-world electronic voting systems. In *Proceedings of the International Symposium on Software Testing and Analysis, Seattle, WA*, July 2008. http://www.cs.ucsb.edu/~seclab/projects/voting/issta08_voting.pdf.
- [5] Nancy Bickel, Judy Bertelsen, David Wagner, et al. Counting our votes on paper and electronically: The League of Women Voters observes the election process in Alameda County in the November 2006 General Election prepared for the alameda county registrar of voters election advisory committee. League of Women Voters of Berkeley, Albany, Emeryville, June 2007. <http://lwvbae.org/ACC\%20-\%20Proposed\%20Practices\%206-26-07.pdf>.
- [6] Harvie Branscomb. AUDIT report to satisfy Colorado Revised Statutes. Election Mathematics Web site, 2008. A report of the audit of the Eagle County, Colorado Nov. 4, 2008 General Election <http://electionmathematics.org/em-audits/CO/2008/AUDITReportEagleCountyC02008.pdf>.
- [7] Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. In defense of pseudorandom sample selection. Center for Information Technology Policy and Dept. of Computer Science, Princeton University Woodrow Wilson School of Public and International Affairs, August 2007. http://www.usenix.org/event/evt08/tech/full_papers/calandrino/calandrino_html/.

- [8] California Secretary of State Debra Bowen’s Office of Voting Systems Technology Assessment. Report to the Election Assistance Commission concerning errors and deficiencies in Diebold/Premier GEMS Version 1.18.19. California Secretary of State Web site, March 2009. http://www.sos.ca.gov/elections/voting_systems/sos-humboldt-report-to-eac-03-02-09.pdf.
- [9] Connecticut Citizen Audit Coalition. Aug 08 primary election observation report. Connecticut Citizen Audit Coalition Web site, October 2008. <http://www/CTelectionAudit.org/Reports/ObservationReportAug08.pdf>.
- [10] Connecticut Citizen Audit Coalition. Feb 08 Presidential Primary Observation Report. Connecticut Citizen Audit Coalition Web site, April 2008. <http://www.ctelectionaudit.org/Reports/ObservationReportFeb08.pdf>.
- [11] Connecticut Citizen Audit Coalition. Nov 07 municipal elections audit observation report. Connecticut Citizen Audit Coalition Web site, January 2008. <http://www.ctelectionaudit.org/Reports/AuditObservationReport.pdf>.
- [12] Connecticut Citizen Audit Coalition. Report and feedback November 2008 Connecticut post-election audit observation. Connecticut Citizen Audit Coalition Web site, January 2009. <http://www.ctelectionaudit.org/Reports/Nov2008/ObservationReportNov08.pdf> Executive Summary http://www.ctelectionaudit.org/?page_id=53.
- [13] Arel Cordero and David Wagner. Replayable voting machine audit logs. Electrical Engineering & Computer Sciences — EECS at UC Berkeley, 2008. <http://www.eecs.berkeley.edu/~arel/replayable-evt08.pdf>.
- [14] Arel Cordero, David Wagner, and David Dill. The role of dice in election audits. University of California at Berkeley Web site, June 2006. <http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf>.
- [15] Center For Democracy and Election Management. Building confidence in US elections — Report of the Commission on Federal Election Reform. American University, September 2005. http://www.american.edu/ia/cfer/report/full_report.pdf.
- [16] Citizens For Democracy. SRV citizen observation reports, riverside county, california. Citizens for Democracy Web site, 2006–2008. <http://cfdtv.netrootz.com/>

web_pages/view_web_page.asp?Group=207\&Page=494 or <http://www.savervote.comandclickonSRVCitizenObservationReports>.

- [17] Deputy Secretary of State Anthony Stevens. Hand counting using on-going verification. Office of the Secretary of State of New Hampshire, 2007. <http://utahcountvotes.org/legislature/NH-Manual-Counting/Hand-Counting-and-Ongoing-Verification.ppt>.
- [18] David Dill. David dill's testimony before the Commission on Federal Election Reform (The Carter-Baker Commission), American University, Washington, DC. Verified Voting Foundation Web site, April 2005. <http://www.verifiedvotingfoundation.org/article.php?id=5987>.
- [19] Kathy Dopp. Utah's new election audit and recount procedures found lacking by Utah's Desert Greens Party and Utah Count Votes. US Count Votes Web site, October 2006. <http://utahcountvotes.org/litgov/Response2LtGov-Audit-Recount.pdf>.
- [20] Kathy Dopp. The history of confidence election auditing development (1975 to 2008) & overview of election auditing fundamentals. US Count Votes Web site, October 2007-2008. <http://electionarchive.org/ucvAnalysis/US/paper-audits/History-of-Election-Auditing-Development.pdf>.
- [21] Kathy Dopp. Checking the accuracy of election outcomes — post-election audit sample sizes. working paper not published yet, April 2009.
- [22] Kathy Dopp and Ron Baiman. How can independent paper audits ensure election integrity? US Count Votes Web site, June 2005-2006. http://electionarchive.org/ucvAnalysis/US/paper-audits/Paper_Audits.pdf.
- [23] Kathy Dopp and Frank Stenger. The election integrity audit. US Count Votes Web site, September 2006. <http://vote.nist.gov/ElectionIntegrityAudit.pdf>.
- [24] Kathy Dopp and Joycelynn Straight. Mandatory vote count audit — A legislative & administrative proposal. US Count Votes and Utah Count Votes Web site, 2006-2008. <http://electionarchive.org/ucvAnalysis/US/paper-audits/legislative/VoteCountAuditBillRequest.pdf>.
- [25] Stephen N. Goggin and Michael D. Byrne. Comparing the auditability of optical scan, Voter Verified Paper Audit Trail (VVPAT) and video (VVVAT) ballot systems.

- USENIX: The Advanced Computing Systems Association*, 2008. http://www.usenix.org/events/evt08/tech/full_papers/goggin/goggin_html/.
- [26] Joseph Hall. Contractual barriers to transparency in electronic voting. Web site, 2008. http://josephhall.org/papers/jhall_evt07.pdf.
- [27] Joseph Hall. Dice binning calculator for post-election audits. Web site, March 2008. <http://www.josephhall.org/dicebins.php>.
- [28] Joseph Hall. *Policy Mechanisms for Increasing Transparency in Electronic Voting*. PhD thesis, University of California at Berkeley, December 2008. <http://josephhall.org/papers/jhall-phd.pdf>.
- [29] David Jefferson, Elaine Ginnold, Kathleen Midstokke, Kim Alexander, Philip Stark, and Amy Lehmkuhl. Evaluation of audit sampling models and options for strengthening California's manual count. California Secretary of State Debra Bowen. Post-Election Audit Standards Working Group, July 2007. http://www.sos.ca.gov/elections/peas/final_peaswg_report.pdf.
- [30] Douglas W. Jones. Auditing elections. *Communications of the ACM*, 47(10):46–50, October 2004. <http://doi.acm.org/10.1145/1022594.1022622> <http://www.cs.uiowa.edu/~jones/voting/cacm2004.shtml>.
- [31] M. Lindeman et al. Principles and best practices for post-election audits. Web site, September 2008. http://electionaudits.org/files/bestpracticesfinal_0.pdf.
- [32] Neal McBurnett. CO election auditing project — auditable reports for Hart Intercivic and Hart CCOS machines). Web site, 2008. <http://bcn.boulder.co.us/~neal/elections/boulder-audit-08-11/>. Contains links to programs to calculate the sample size, and randomly select the sample and the contests to audit at <http://bazaar.launchpad.net/~nealmcb/electionaudits/trunk/files>, <http://bcn.boulder.co.us/~neal/electionaudits/>.
- [33] Walter R. Mebane, Jr., Jasjeet S. Sekhon, and Jonathan Wand. Detecting and correcting election irregularities. Stanford University Web site, October 2003. <http://wand.stanford.edu/research/detecting.pdf>.
- [34] Lawrence Norden, Aaron Burstein, Joseph Lorenzo Hall, and Margaret Chen. Post-election audits: Restoring trust in elections. Brennan Center for Justice with the Samuelson Law, Technology & Public Policy Clinic, August 2007.

http://www.brennancenter.org/dynamic/subpages/download_file_50227.pdf
Executive Summary http://www.brennancenter.org/dynamic/subpages/download_file_50228.pdf http://www.brennancenter.org/dynamic/subpages/download_file_50109.pdf.

- [35] Lawrence Norden and Eric Lazarus. The machinery of democracy: Voting system security, accessibility, usability, and cost. The Brennan Center for Justice Web site, 2006. http://brennan.3cdn.net/cb325689a9bbe2930e_0am6b09p4.pdf.
- [36] Ronald L. Rivest. A Sum of Square Roots (SSR) pseudorandom sampling method for election audits. MIT Web site, April 2008. <http://people.csail.mit.edu/rivest/Rivest-ASumOfSquareRootsSSRPseudorandomSamplingMethodForElectionAudits.pdf>.
- [37] Pamela Smith. Written testimony of Pamela Smith, President, VerifiedVoting.org before the Committee on House Administration, Subcommittee on Elections, U.S. House of Representatives. Web site, March 2007. http://electionaudits.org/files/PamelaSmithTestimonyFinal_2007mar20.pdf.
- [38] Philip B. Stark. CAST: Canvass Audit by Sampling and Testing. Department of Statistics, University of California, Berkeley, August 2008. <http://statistics.berkeley.edu/~stark/Preprints/cast08.pdf> and <http://www.stat.berkeley.edu/~stark/Seminars/ksu08.pdf>.
- [39] Philip B. Stark. Election audits by sampling with probability proportional to an error bound: dealing with discrepancies. Department of Statistics, University of California, Berkeley, 2008. <http://statistics.berkeley.edu/~stark/Preprints/ppebwrwd08.pdf>.
- [40] Philip B. Stark. A sharper discrepancy measure for post-election audits. *The Annals of Applied Statistics*, 2(3):982–985, 2008. <http://statistics.berkeley.edu/~stark/Preprints/pairwise08.pdf>.
- [41] The Election Audits Task Force. Report on election auditing, January 2009. http://www.lwv.org/Content/ContentGroups/Membership/ProjectsTaskforces/Report_ElectionAudits.pdf.

- [42] US General Accounting Office. Federal efforts to improve security and reliability of electronic voting systems are under way, but key activities need to be completed. US GAO Web site, 2005. <http://www.gao.gov/new.items/d05956.pdf>.
- [43] Paul Walmsley. Requirements for statistical live auditing of optical-scan and VVPAT records — and for live auditing for vote tabulation. Web site, 2005. <http://www.booyaka.com/~paul/ea/eac-20050930/live-audit-overview.txt> <http://www.booyaka.com/~paul/ea/eac-20050930/interpretation-live-audit.txt> <http://www.booyaka.com/~paul/ea/eac-20050930/tabulation-live-audit.txt>.
- [44] Jonathan Wand. Auditing an election using sampling: The impact of bin size on the probability of detecting manipulation. Stanford Web site, 2004. <http://wand.stanford.edu/elections/probability.pdf>.
- [45] David R. R. Webber. Trusted logic voting systems with OASIS Election Markup Language 4.0. Open Voting Solutions Web site, January 2007. <http://openvotingsolutions.net/material/Trusted%20Logic%20Voting%20Brief.pdf> and <http://www.oasis-open.org/committees/download.php/30366/EML-Top-Reasons.pdf>.