Using automatically created digital ballot images to verify voting-machine output in Wisconsin

A Citizens' Report on the
Development of a Slide-Show Verification Method

Wisconsin Election Integrity Action Team
Karen McKim, Coordinator
January 2016

WisconsinElectionIntegrity.org

Summary

The Problem: **Computer output is occasionally flawed, yet Wisconsin elections officials do not routinely verify voting-machine output.** No computer is completely immune to errors, and vote-tabulating computers are no exception. That is not a problem when the computers' verdict is verified before election results are declared final. However, Wisconsin elections officials verify the correct winners in only a small fraction of our electoral contests--those with results so close the loser demands a recount. The outcomes in all other races are declared final on the basis of computer output that no one has checked for accuracy.

In no other use of computers in business or government do we tolerate such consequential and unquestioned use of unaudited computer output; elections administrators are alone in having no routine way of noticing computer errors.

The Solution: **Routinely verify the accuracy of voting-machine output.** Wisconsin statutes require a paper record of every ballot so that local election clerks can verify output. But currently none do. Clerks give two pragmatic reasons for certifying unaudited output: Available time and a desire to leave the paper ballots sealed for security.

Drawing upon the recommendations and work of national election-administration experts, the Wisconsin Election Integrity Action Team has developed a method for verifying output that resolves both these issues:

- **Verification can be accomplished in a fraction of the time of a recount.** Wisconsin election clerks' only experience with anything resembling post-election verification has been full recounts conducted under s.9.01. Wis. Stats., and biennial voting-machine audits required by s.7.08(6), Wis. Stats, both of which require time-consuming hand counts of every vote on every ballot and resolution of every ambiguously marked vote. The method described in this paper makes use of statistical sampling techniques endorsed by national elections experts, known as risk-limiting audits, which confirm only the outcomes (that is, Who won?), without confirming exact vote totals.
- **Marked paper ballots can remain sealed and untouched.** Wisconsin election clerks are strongly averse to accessing paper ballots after they have been sealed on Election Night. The method described in this paper relies not upon the paper ballots, but upon digital images created by the voting machines as the ballots were cast. The actual ballots can remain sealed unless anomalies are detected during review of the digital images. Although using digital images introduces certain additional concerns about the accuracy of the audit record (as opposed to paper ballots), counting votes from the digital images is much quicker than using paper ballots, because it eliminates substantial paper-handling and allows several independent counts to be performed simultaneously as digital images are projected like a slide show.

The procedure in brief: Before the election, the clerk needs to develop and publicly promulgate procedures for selecting the races to be audited, to avoid the appearance of auditing only those outcomes he or she doesn't like. The goal of the procedure should be to verify that the correct winner(s) were identified, not simply that a few machines counted accurately.

On Election Day, a digital image of each ballot is automatically saved by the voting machine at the moment each voter inserts his or her ballot. For security purposes, elections clerks should make multiple copies of the digital-image files as soon as possible after poll closing. After Election Day, the necessary sample sizes are calculated and samples drawn, as transparently as possible.

To verify the electronically tabulated election results, the digital images are projected as a slide show so that official counters and public observers can count votes simultaneously. Each person counts votes for only one candidate. An operator begins a slide show in which each ballot is projected for two seconds or less, depending upon the preference of the auditors.

After 25 ballots are projected, the slide show automatically pauses so that counters can compare their count for that batch. If they agree, the subtotal is recorded on a tally sheet. If they do not agree, the same 25 ballot images are projected again so that the discrepancy can be resolved or identified.

If the audit is being performed on an entire precinct, the subtotals from each batch are tabulated after all ballots from that precinct have been viewed, and are compared against the total tabulated by the voting machine.

If the audit is being performed on a statistical sample, the subtotals are tabulated after votes have been counted from the sample, and auditors calculate the probability that a full hand count would identify the same winner(s) identified by the electronic tabulation, given the results from the sample. The vote-counting can end as soon as the electronically tabulated outcome is confirmed to a pre-determined level of statistical certainty (such as 99.9%).

If the results of the sample do not confirm the electronically tabulated winners, local policy will need to determine the next steps: The sample could be expanded with additional randomly selected ballots until an outcome is confirmed, or the exercise could be halted and replaced with a full hand recount of the paper ballots.

The Conclusion: **The County Clerk should develop official slide-show verification procedures and adopt them as a routine part of the county canvass.** Use of these procedures during the canvass process would achieve significant improvement in the integrity of Wisconsin elections with minimal additional cost or time, compared to current practices.

Compared to hand counts, the slide-show verification process has advantages (much more efficient and transparent counting) and a drawback (chain-of-custody for digital images is less transparent than that for paper ballots). Risk-limiting auditing has efficiency advantages over full recounts regardless of whether paper ballots or digital images are used, and has the drawback of answering only one question—Did we identify the right winner?—without necessarily providing information about the accuracy of any specific machines. Additionally, some skeptical voters will never be convinced by conclusions drawn from samples or by anything short of a full hand count of paper ballots.

Contents

The Basic Why and How of Verification

1. Computer output should be verified.

As the polls close on Election Day, we can never be sure we have successfully protected our voting machines against accidents and unauthorized programming. Even successfully pre-tested machines can miscount on Election Day. Voting-machine output, like that of other computers, can be unexpectedly and randomly impaired by:

- Human error—Electronic miscounts have been caused by programming errors (e.g., the 'Deck-Zero' problem discovered in Humboldt County[i]); or by set-up errors.[ii] Additional errors in pre-election testing have caused programming and set-up errors to go undetected before Election Day.[iii]
- Mechanical or electrical malfunction—Electronic miscounts have been caused by electrical and mechanical malfunctions[iv], and by maintenance issues such as dust and dirt[v] interfering with correct operation; and
- Deliberate sabotage by insiders or external hackers[vi]. High-profile hacking incidents affecting companies with IT security programs as strong as those of Anthem Health, Sony, Target, the Federal Reserve Bank, and the US Office of Personnel Management should alert us to the fact that our elections officials and voting-machine companies will have little chance against hackers or corrupt insiders when they decide to determine the outcomes of our elections.

Although even the most diligent local elections clerk cannot protect ***preliminary*** election results (that is, the voting-machine output) from all those risks, we can still protect ***final*** election results by verifying the voting-machine output against the evidence on the ballots before certifying results.

National elections administration experts, including the 2014 Presidential Commission for Elections Administration[vii], the Brennan Center for Justice[viii], and the national League of Women Voters[ix], unanimously recommend routine post-election verification of electronically tabulated election results.

2. Election audits present unique challenges.

Elections official must 'certify' election results—that is, declare them final—within a few weeks after each election. After election results are certified, they are no longer subject to recount or challenge. Therefore, unlike computer-generated bank or credit-card statements, for which errors can be reversed even when discovered several months later, voting-machine output must be audited promptly if errors are to be corrected.

Unfortunately, many techniques used to verify most other computer applications are not possible with elections. The privacy of the ballot prevents us from giving voters any kind of receipt that could confirm their votes were correctly tallied with their neighbors', and because private audit firms are just as interested in the election outcomes as anyone else, none are independent enough to be trusted with producing or verifying election results.

Instead, election audits must rely on transparency to ensure impartiality. Fortunately, national experts in both elections administration (e.g. Brennan Center for Justice, Verified Vote Foundation) and in other fields (e.g., American Statistical Association, Argonne National Laboratory) have contributed their efforts, and substantial guidance is available to any elections clerk who wants to verify the output of his or her voting machines.

3. Wisconsin law allows prompt verification, but it is not done.

Wisconsin's election officials—specifically, county clerks and county boards of canvass—have statutory responsibility to ensure the accuracy of our election results. They undertake responsible pre-election measures to maintain security, and our observations of poll closings and municipal canvasses have provided us with confidence that Wisconsin's municipal officials do a timely and reliable Election-Night job of confirming that the voting machines counted the correct number of ballots (though not votes), a necessary first step in post-election verification.

Wisconsin statutes anticipate verification by requiring voting machines that use voter-marked paper ballots or that create a "paper audit trail," consisting of a machine-printed paper record of every ballot. In addition, the county board of canvass has wide statutory leeway for the processes it will use to canvass (review) the preliminary results, and has clear authority to direct municipalities to correct any observed informalities or defects with the preliminary results.[x]

After election results are declared final, however, statutes contain no provision for correction, so verification needs to be timely.

However, most county election officials currently resist verification. Much of this resistance is based on misconceptions about their ability to prevent Election-Day miscounts:

- Some officials mistakenly believe that federal and state certification of commercial elections systems ensure that individual machines cannot miscount. For example, the chairman of the Wisconsin Government Accountability Board was challenged at a legislative hearing in October 2015 regarding that agency's failure for several years to order municipalities to conduct post-election audits. The chairman testified that he was unconcerned about the lack of audits because he believed the original certification tests sufficiently established the voting machines' reliability.
- Some officials mistakenly believe that pre-election testing can protect against or detect miscounts, when in fact they cannot detect miscounts caused by Election-Day malfunction or deliberate mis-programming. For example, a Wisconsin county clerk wrote in July 2015 that post-election verification is "unnecessary" because his office runs "hundreds of marked ballots through the DS200 with all types of permutations where we know beforehand what the result should be when the result tapes are printed. … The municipal clerks then separately run their own set of ballots through the DS200's as part of their public testing. This acts as a check against our testing, a second check on the tabulator, and it instills confidence in an open-meeting format that the equipment is properly tabulating votes."
- Other misconceptions provided as reasons certifying unverified output include:
  - Accurate results in previously recounted races are believed to indicate reliability in future elections. In fact, accurate performance in past elections cannot predict, prevent, or detect subsequent miscounts.
  - Voting machines that are not connected to the Internet while the machines or software are in the clerks' possession cannot be hacked. In fact, the clerks have no control of the security of the software and hardware while it is in the possession of the vendor or when the vendor installs required patches and updates; the clerks do not routinely verify that no one has installed wireless communications capability on their voting machines; and Internet connections are not required for insider fraud.

- Many clerks believe that because they are unaware of any previous miscounts related to the type of machine they use, no miscounts have occurred or will occur. In fact, clerks are not routinely informed when miscounts occur in other jurisdictions, and in any event miscounts are not likely to be discovered when verification is not routinely performed.
- Many clerks believe that Wisconsin's practice of spot-checking several dozen voting machines biennially is sufficient to deter or detect any significant miscounts. In reality, these audits have multiple methodological limitations that render them unable to detect even significant miscounts, including small sample size and an instruction that auditors are to disregard any miscounts attributable to human error or action, including mis-programming[xi],

Two other issues provide more reasonable basis for county clerks' resistance to verification: Available time and the desire to maintain security for the paper ballots.

Time - Wisconsin's county clerks have a limited amount of time between Election Day and when they must certify election results as final. Statutory certification deadlines vary depending on certain contingencies, but roughly speaking, county clerks have about three weeks after Election Day to certify results in non-recounted races. Candidates and news media usually pressure them for even earlier certification. Therefore, an acceptable verification procedure needs to be able to be completed in just a few working days.

County clerks could verify results ***after*** certification, but Wisconsin statutes contain no provision for correcting errors discovered after certification, so discovery that the clerk certified miscounted results would cause intolerable scandal, bitter controversy, and expensive litigation.

Security for the paper ballots - Most clerks also express fear of opening sealed ballot bags, despite having the skills and authority to preserve security when they open and reseal ballot bags. When no races are going to be recounted, prohibiting audits to protect ballot security is irrational, because the security procedures are instituted for the sole purpose of enabling valid audits. If the ballots are never used for audits, the security serves no function. Nonetheless, the clerks' resistance to accessing sealed paper ballots is very real and needs to be taken into account.

4. Output could be verified efficiently.

The Wisconsin Election Integrity Action Team, a volunteer citizens group supported by the Wisconsin Grassroots Network, believes that county clerks would like to ensure accurate election results, and would do so if provided with practical, economical, and efficient verification procedures and with interest from the voters and candidates they serve. The former state Government Accountability Board did not have responsibility for developing such procedures, and did not do so.

The Election Integrity Action Team began developing an efficient verification system consistent with existing Wisconsin statutes in early 2015, when we obtained a complete set of digital images of ballots cast in the February 17 nonpartisan primary in Dane County, Wisconsin from that county's clerk. This system is designed to be used by county clerks during the two-week period following each election that culminates with the county board of canvass signing a certification statement attesting to the fact that the results are "correct and true."

The system is called a 'slide-show verification system' to distinguish it from a hand count. It is like a hand count insofar as election officials and citizens, not computer programmers, count the votes. It is unlike a hand count insofar as human eyes rather than human hands do most of the work. Attachment A contains a side-by-side comparison of the benefits and limitations of this method of verification, as compared to hand counting paper ballots.

The astounding benefit of slide-show verification, when compared to hand counts of paper ballots, is speed. When two teams of two auditors (four people) counted votes for two candidates in a mayoral primary, they reached agreement on the visual count for both candidates at a rate of 125 ballots every five minutes, so that a reporting unit with 1,000 ballots could be verified in 40 minutes. A hand count of the same precinct would have taken the same number of people at least two hours.

This remarkable time savings came from enabling both members of each pair of auditors to count simultaneously instead of consecutively (cuts the time in half); eliminating the chain-of-custody procedures surrounding unsealing and resealing ballot bags; eliminating the paper-handling and moving (ballot counting and stacking, moving the ballots while counting); freeing up the inspector's hands to enable them to use a clicker-counter; and enabling them to keep their visual focus on the screen instead of looking back and forth between a ballot and a tally sheet.

The verification system described in this report is still in development. At this writing (January 2016), it has been tested only three times, twice using random samples of City of Madison reporting units in a February 17 five-candidate mayoral primary, and once using a single entire precinct in an April 7 yes-no referendum. The purpose of this document is to share information about the progress to date in the hopes of eliciting constructive comments and suggestions, guidance, and support from knowledgeable readers, which can be submitted to WisconsinElectionIntegrity@gmail.com. A list of unresolved questions and issues is Attachment B.

The digital ballot images

In recent years, Wisconsin elections officials have been purchasing electronic voting systems that are capable of saving a digital image of each voter-marked paper ballot. Two such systems—the ES&S DS200 and the Dominion Voting Imagecast Precinct system—are approved for use in Wisconsin. The digital images preserved by these systems provide the opportunity to verify electronically counted election results without accessing the sealed paper ballots.

These voting systems create the digital images not as an optional feature, but as a necessary step in detecting the votes on each ballot. Technically, the system is not an optical scanner—that is, it does not rely on photosensors to detect light reflected off the ballot. Instead, these machines count votes by creating a pixelated image of each ballot, which it then analyzes to discern and count the votes. Depending upon how the machine is set up, it can either discard the digital image when it has interpreted and recorded the votes, or it can save the image. Setting the machine to preserve the images is the first step whenever any clerk wants to use the digital images for security or verification. Wisconsin's Government Accountability Board has required local elections clerks to set the machines up to preserve the digital images.

Although they are not the official legal record of each ballot, the digital images enhance the security of the election record in several ways. In voting machines with unadulterated software that has been correctly set up and is working correctly, a true, clear image of the ballot is created immediately when the voter inserts it into the machine. This has a deterrence value against certain types of election fraud in jurisdictions that routinely verify voting machine output, because it requires an election thief to alter three things: the actual ballots, the digital images of those ballots, and the tabulated results. Without routine verification, of course, there is no deterrence value to either the paper ballots or their digital images, because the electronic tabulations will never be checked against them.

The digital image files can also be copied quickly (compared to manually scanning the ballots) at very low cost, providing diligent county clerks with the opportunity to make multiple copies of the record. These multiple copies, if made available to independent auditors or potential auditors, create another layer of deterrence for any attempts to alter the record of the votes.

And of course, the digital images can be viewed with no risk to the security of the voter-marked paper ballots themselves. It is this feature that makes the slide-show verification method most attractive to clerks who are concerned about keeping the paper ballots continuously sealed until their destruction.

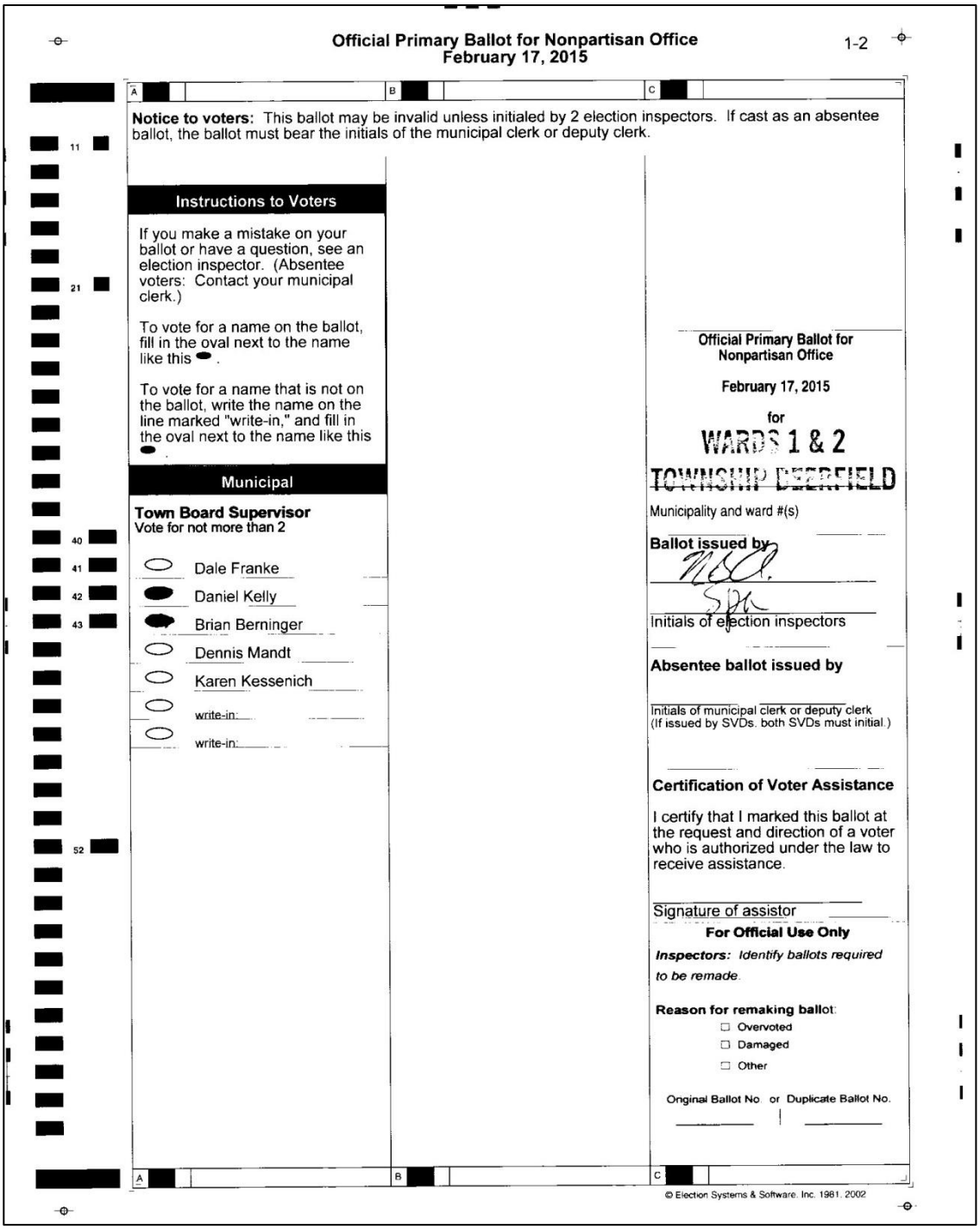
On ES&S's DS200, the only system we have worked with, a single flash drive contains the digital ballot images, election set-up instructions, the event record, and the tabulated totals. On Dominion's Imagecast Precinct, the digital images are stored on a separate flash drive.

On the DS200 system, each ballot is saved on two separate files within one electronic folder, each with a unique 39-digit file name (e.g., N0001300000DS01133901674c5c9bb75003349F.pbm.zip is the front of a ballot, and N0001300000DS01133901674c5c9bb75003349R.pbm.zip is the reverse side of the same ballot.) Files with the extension .pbm are 'portable bitmap images', a digital-image file type designed in the 1980s to be easily exchanged between platforms.

The images use only black and white pixels—no gray. This can create odd patterns in areas of the ballot with gray shading, but did not interfere with our ability to discern votes.

The images provided to us in the February and April elections had a high resolution of 3.8 million pixels per ballot. The voting-machine manufacturer has not yet responded to questions regarding whether the resolution is variable. An actual ballot image created by the DS200 is reproduced on the following page.

During our two tests, we viewed ballots from approximately two dozen reporting units and saw none that were illegible. In our random sample of precincts, we noted no reporting units in which the number of saved ballot images appeared to be different than the number of ballots cast on Election Day, judging from the number of votes electronically recorded in each precinct.



Official Primary Ballot for Nonpartisan Office
February 17, 2015

1-2

Notice to voters: This ballot may be invalid unless initialed by 2 election inspectors. If cast as an absentee ballot, the ballot must bear the initials of the municipal clerk or deputy clerk.

Instructions to Voters

If you make a mistake on your ballot or have a question, see an election inspector. (Absentee voters: Contact your municipal clerk.)

To vote for a name on the ballot, fill in the oval next to the name like this ●.

To vote for a name that is not on the ballot, write the name on the line marked "write-in," and fill in the oval next to the name like this ●.

Municipal

Town Board Supervisor
Vote for not more than 2

- ○ Dale Franke
- ● Daniel Kelly
- ● Brian Berninger
- ○ Dennis Mandt
- ○ Karen Kessenich
- ○ write-in:
- ○ write-in:

Official Primary Ballot for Nonpartisan Office

February 17, 2015

for

WARDS 1 & 2

TOWNSHIP DEERFIELD

Municipality and ward #(s)

Ballot issued by

Initials of election inspectors

Absentee ballot issued by

Initials of municipal clerk or deputy clerk
(If issued by SVDs, both SVDs must initial.)

Certification of Voter Assistance

I certify that I marked this ballot at the request and direction of a voter who is authorized under the law to receive assistance.

Signature of assistor

For Official Use Only

Inspectors: *Identify ballots required to be remade.*

Reason for remaking ballot:

- ☐ Overvoted
- ☐ Damaged
- ☐ Other

Original Ballot No. or Duplicate Ballot No.

This image provides a rough indication of the resolution preserved on the digital ballot images in the two elections for which we have images. The image above was created by a City of Madison DS200 machine on February 17, 2015, copied to the county clerk's computer, copied to a flash drive, and converted to .jpg to make it possible to copy it into a Word document. It was reduced in size to fit on one page. Actual resolution when viewed directly on a computer monitor is higher.

We have yet to determine the reliability of the digital-image preservation function. We did not check the February files for missing images, although the Dane County clerk's office reported that one of their staff

was unable to locate all the digital images for the City of Fitchburg. In the April 2015 elections, the Village of Black Earth did not preserve the digital images. We have not yet received a response to our questions to the Dane County Clerk regarding why the images were not preserved and how complete election records can be ensured in the future.

Finally, the DS200 system does not provide an easy way to match individual digital images with an actual paper ballot, and it is likely Wisconsin clerks—until they acknowledge the need to verify their voting machines' accuracy—will resist opening ballot bags to check the accuracy of the digital images.

See page 13 for a discussion of the issues related to digital images as audit records.

Risk-limiting auditing

Risk-limiting auditing is a technique that enables election auditors to reach reliable conclusions about the accuracy of the voting-machine output by counting votes from only a sample of ballots, rather than from all ballots. Risk-limiting audits count a sample only large enough to determine only whether the electronic tabulation identified the correct outcome. That is, while a ***recount*** would verify that the electronic tabulation was correct in recording 13,457 votes for Candidate Washington and 12,001 votes for Candidate Adams, a ***risk-limiting audit*** would seek only to determine with a high level of confidence that the electronic tabulation correctly identified Washington as the winner.

A typical flat-percentage audit requirement, e.g., 1% of all precincts; 3% of races, etc., may not count enough ballots when true results are close and therefore fail to detect miscounts—particularly in the absence of any requirement to expand the sample when discrepancies are found—and may force elections officials to count more ballots than necessary when true results are not close.

In a risk-limiting audit, an initial sample size is calculated for each race to be audited, taking into account several factors including the number of ballots cast and the size of the electronically tabulated victory margin. The sample can include entire precincts, or can draw ballots randomly across the entire jurisdiction, although samples designed to include entire precincts will need to be larger.

After votes are counted from the initial sample of ballots, auditors use the results to calculate the probability that a complete hand count would identify the same winner(s) as the electronic tabulation. If the probability is 99.9% or higher, the risk-limiting audit is complete and has verified the accuracy of the electronic count. If, however, results from the sample indicate a lower probability that a full count would identify the same winner(s) as the electronic tabulation, the size of the sample is increased and additional ballots are counted. The process continues until the audit has established that the electronic tabulation identified the correct outcome, or has recounted all the ballots and identified a different outcome.

Because a recount using the digital images would likely not be accepted as a definitive legal count of election results, we believe that when Wisconsin clerks use risk-limiting audits with digital ballot images, they should adopt a policy of suspending the digital-image audit if the initial samples do not confirm the electronically tabulated totals and begin a full hand count of the actual paper ballots for the questioned race.

We were unable to obtain consultation from a trained statistician to assist us in performing a true risk-limiting audit for our first tests, which limited the extent to which we can comment from first-hand experience and highlights one drawback of this method. Although statistically valid methods provide great efficiency in allowing election clerks and auditors to count many fewer ballots than they would otherwise need to while still providing high levels of assurance that election results are correct, the

calculation of the correct sample sizes requires credible statistical expertise. The formulas used in risk-limiting auditing have been developed, tested, and published by the American Statistical Association[xii], so a statistician would need only to apply them, but the credibility of the process would depend upon having a trained statistician to ensure that the calculations were done correctly.

The Slide-Show Verification System, step by step

The following section provides a description of the slide-show verification system as we believe it could be implemented in Dane County, Wisconsin. Some steps cannot be performed by citizens' groups, so citizen audits will be unable to achieve the reliability and credibility possible with an official verification. As noted, the procedure should still be considered in development; refinements and improvements are likely possible for any of the following steps.

1. Announcing the process and criteria for sample selection

For protection against accusations of selecting contests for verification based on whether the clerk liked the outcome, the clerk must before the election make known the criteria and process for selection of contests and precincts to be audited and the method by which the sample size will be determined. The process should use risk-limiting auditing, to reflect currently accepted best practices for post-election verification.

The clerk should take steps to ensure that all municipalities have set the machines up correctly to preserve ballot images.

2. Submission of digital images to the county clerk

In Dane County on Election Night as part of poll-closing procedure, the preliminary vote totals—but not the digital images—are electronically transmitted to the county clerk's office. The flash drive containing the digital ballot images is removed from the voting machine at each polling place and is manually transported to the clerk's office in a zipper bag locked with an initialed seal, along with the other election records. Elapsed time between poll closing and the delivery of election records to the clerk's office is an issue for chain-of-custody, affecting both the paper ballots and the flash drives, particularly if the election records are stored overnight or unattended at any point before delivery to the county clerk.

When the flash drive arrives at the county clerk's office, its contents are copied to the county clerk's computer. We do not know from first-hand observation, but have been told that the elections computer is never connected to any other or to the Internet. Each precinct's ballot images are saved in a separate folder.

3. Making security copies of the digital-image files

As soon as all precincts' images have been copied to the clerk's computer, the clerk should make multiple copies of the full set of ballot-image files. For his or her own protection, the clerk should make these copies as soon as possible, because the longer the time during which the clerk has sole possession of the digital images, the more opportunity he or she will have to tamper with the images or to be accused of tampering. Prompt duplication and distribution of the digital-image files to independent parties is a strong security measure, because making hard-to-detect alterations to the digital-image files would take much longer than altering the numerical tabulations alone.

Each political party with a candidate on the ballot should receive a copy of the digital image files, as should the newspaper of record for the county and any citizen's group that has requested one.

4. Verify that the number of digital images matches the number of ballots cast.

If it does not, determine why the digital images were missing. If possible, obtain the missing digital images and provide copies for those who received the digital-image files. If the images were not saved, determine the effect of the missing files on the validity of the planned verification.

5. Conduct the public display of ballots for transparent vote-counting

At the time and place announced for the public verification of the election outcomes, one of the flash drives with the ballot images is plugged into a computer loaded with the software that can project the ballot images as a slide show on a wall screen.

The slide-show software and display

- The slide-show software was developed specifically for this purpose by a member of the Wisconsin Election Integrity Action Team who is a professional Microsoft programmer. It is open-source software; copies are available upon request from WiscElectionIntegrity@gmail.com.
- The software makes no changes to the digital-image files; it merely reads and projects them.
- The software is designed so that the projected image can be adjusted to include the entire ballot, front and back or any area on either side, so the slide show can focus on only one race or several.
- As each ballot is displayed, a bar at the top of the screen displays a number, e.g., 'Ballot 341 of 412,' and the ward/precinct, e.g., 'City of Madison Ward 16.'

The auditors (the official counters) and observers

- Ideally, some of the elections inspectors who had initialed the ballots will be present, because they will be able to examine and confirm their initials on the ballot images.
- A team of two official inspectors should be assigned to each candidate whose votes will be counted. They should sit in front facing the screen with hand-held clicker counters. They should be seated far enough apart, however, that they cannot discern the sound of the click made by their teammate's counter.
- Any number of public observers can be present and counting along. Public observation of the count lends powerful credibility to the process and to the integrity of the election results.

Checking the number of ballots

If counting for a full reporting unit (precinct, ward), the file directory for the flash drive is projected, the folder for the randomly selected precinct is displayed, and the number of ballot images in that folder is compared to the number of ballots reported to have been electronically tabulated at that precinct. The numbers should match. If not, it indicates a problem that must be resolved before verification is possible with the digital images. If the problem cannot be resolved, verification with the paper ballots is necessary. We encountered no such problem during our tests.

Checking the ballot images for obvious signs of alteration

The first few ballots in each precinct's folder are projected and examined for signs of alteration or substitution—do the voters' marks look natural and normally variable? Are the poll workers' initials appropriate and natural-looking? If not, it indicates a problem that must be resolved before verification is possible with the digital images. If the problem cannot be resolved, verification with the paper ballots is necessary. We encountered no such problem during our tests.

Counting the votes

Starting with the first ballot in the precinct or sample, the ballots are individually projected at a variable rate of 0.5-2 seconds per ballot. In our tests, we found that one second per ballot was best speed. We achieved accuracy more readily at that speed than at two seconds per ballot.

The slide show automatically pauses after every 25 ballots, and the two members of each team compare their subtotals for that batch of 25 ballots. If there are no discrepancies, the agreed-upon subtotal is recorded and the slide show continues. If the members on any team disagree, the last 25 ballots are displayed again, and everyone in the room counts for the same candidate. If any votes are ambiguous, the number of the ballot is recorded (e.g., Ballot #78 in Ward 34), but no effort is made to resolve the differing interpretations of the vote. When the two official inspectors agree on the count for that batch of 25 or have identified the ballot on which they disagree, the slide show resumes.

Over both demonstrations, we inspected approximately 1,500 ballots and found none on which the official inspectors and audience members disagreed on how the vote should be counted. We found two ballots that contained idiosyncratic marks that we initially questioned whether the machine would have counted as votes, but for which the voter intent was clear for all who were present. Our final counts indicated that the machines had interpreted the votes the same way the auditors had.

When full precincts are counted: When the slide show reaches the end of the precinct, the agreed-upon subtotals are added and compared to the electronically counted totals reported from that precinct on Election Night. If they agree, or if the counts are different and the difference can be explained by the ambiguous votes noted during the counting, that finding is noted on the tally sheet and the verification for that precinct is complete, and verification moves on to the next precinct. If they do not agree, the discrepancy is noted and the verification moves on to the next precinct.

Any findings of discrepancies are reported to the County Board of Canvass, which should then order a prompt hand count of paper ballots to resolve the irregularity before election results are certified, per its authority under s.7.60, Wis. Stats.

If a risk-limiting audit sample is used, vote-counting continues in batches of 25 votes until the sample has been counted. At that time, the consulting statistician calculates the probability that a manual count of all the ballots would identify the same winner as the electronic tabulation. If the probability reaches the previously agreed-upon level (the ASA recommends 99.9%), the audit has confirmed the accuracy of the outcome. If the probability is less than the agreed-upon level, the statistician can calculate the required size of an additional sample, and that can be counted, or the findings could be reported to the County Board of Canvass for decision on further action.

Risks of auditing with digital images

If an audit of election results is to have any value beyond mere appearance, it needs to compare the electronically tabulated election results against a true, accurate, and complete record of the votes. In other words, the record cannot have been replaced by a different record; it cannot have been altered; and no parts can be missing or added.

In addition, that record needs to be ***verifiably*** true, accurate, and complete. Steps must be taken from the moment the record is created to reduce or eliminate damage to the record, and a chain of custody must be documented to demonstrate that those security steps were faithfully performed.

Both paper ballots and digital images have security risks that can ruin their value as an auditable record.

For both paper ballots and digital images, the most important security measure is the most obvious and the most routinely violated: At some point, ***someone must look at the record***. The routine practice of sealing paper ballots on Election Night and retaining them unexamined until their destruction ***creates*** a

security risk, because such complete secrecy provides election thieves with confidence their fraud will not be detected. Each jurisdiction must be known to have some process—however perfunctory—that ensures discerning human eyes might at some point view any record intended to serve an election-integrity purpose.

Beyond that, the risks and countermeasures for paper ballots and digital ballot images are different. If both have been handled appropriately, the original voter-marked paper ballots are the superior record, and audits conducted using those are more credible. However, considerations of ease-of-handling, efficiency, and the reluctance of clerks to access the paper ballots provide arguments in favor of auditing with digital images rather than paper ballots.

The risks to paper ballots are well-known. Paper ballots must be repeatedly handled before being sealed on Election Night. They must be removed from the machine, straightened out, examined for write-in votes, and packaged. Experience has demonstrated risks from accident (valid marked ballots have been left in the machines or elsewhere, or inadvertently discarded) and from deliberate tampering or substitution, which requires access but no specific technical skills. Accidents have destroyed paper ballots or rendered them unusable in other ways. Ballot bags have simply gone missing or have been mishandled in ways that ruined the ballots' suitability as a credible audit record.

The risks to the digital images are different. The digital images are less vulnerable to inadvertent human interference than paper ballots, because they are automatically saved electronically inside the machine; need no human 'handling' after poll closing; and need to be copied only once or twice before verification. However, problems with machine operation or programming may cause the digital images to be garbled or unusable in some way, and deliberate manipulation is possible.

Risk #1: The digital images may not be saved, or the files may be corrupted in some way.
We do not know the reliability of the digital-image preservation function. A few jurisdictions failed to submit digital-image files in either the February or April election. Dane County Clerk Scott McDonell responded to our inquiry by saying he was looking into what went wrong, but has not yet shared his findings. We detected no reporting units in which the number of saved ballot images was different than the number of ballots cast on Election Day, although we did not check them all.

Risk #2: Substitution of falsified digital images for accurate ones
Ballot images prepared before the election could be either pre-loaded into the voting machine or substituted after the polls close, and producing the correct number of ballot images would be a technically easy task. However, deliberate fraudulent substitution would be easy to detect if the jurisdiction views the digital images at any point.

Undetectable substitute ballots would need to have been marked to mimic natural variation in the way voters mark their ballots. In addition, preparation of an undetectable batch of false images would require the thief to wait until the ballot design was finalized to begin the process of creating false images; and would require impossibly accurate forecasting of details such as which poll workers were going to initial the ballots; the handwriting they would use when they did; and the exact precinct-level results in all contests, not just the targeted race in which results will be manipulated.

If an election thief waited until after Election Day, he or she could prepare convincing false images, but the task of preparing the images would take substantial time.

Security measures against substitution:

1. Because of the difficulty of pre-loading convincing fake images into the voting machines or the flash drives, we do not believe any pre-election steps are needed specifically to prevent this remote risk.
2. To prevent substitution after Election Day, we are recommending that county clerks make duplicate copies of the ballot images as soon as they are received in the clerk's office. (The files are large, and after a high-turnout election, copying can be time-consuming.) The duplicate copies should be promptly distributed to at least a few independent recipients, such as political parties, newspaper, or an independent repository that can prevent undocumented access even by the clerk.

Risk #3: Alteration of digital images

On each digital image, properly programmed voting machines can recognize which pixels are votes for which candidates. Unauthorized programming could be inserted to instruct the machine to:

- Cut and paste portions of the digital image, moving the pixels indicating a marked vote to appear beside the desired candidate and moving pixels showing an empty oval to appear beside the candidate the voter actually selected;
- Create additional votes on the digital image without erasing unwanted votes, thus voiding the vote in that race; or
- Erase unwanted votes from the digital image without creating new votes.

If this process is performed before the machines count the votes, it would need to take place quickly as the ballot is processed, in a way that does not detectably slow the voting process.

One natural barrier to this hack is that the unauthorized programming instructions for moving pixels cannot be written until after the ballot design has been finalized, which limits the amount of time a hacker or rogue insider would have to write and insert the unauthorized programming, and in Wisconsin the unauthorized instructions would need to be unique for each jurisdiction.

The likelihood of these manipulations can be assessed only with independent access to the machines and the ability to test them. However, the IT experts with whom we have discussed these possibilities indicate that such manipulation would be difficult; might be easy to detect, and may even be impossible.

First, the voting machines are not likely to be manufactured with extra processing capacity beyond that needed to perform processes beyond the straightforward tasks they are required to perform. Limited processing capacity does not present a barrier to unauthorized programming that simply alters vote totals, but could be a more significant barrier to any hack that requires alteration of digital images. It might be that additional operations of changing the pixels on the ballots would slow the machines noticeably or even cause them to crash or freeze.

Security measures against alteration:

1. The county board of canvass should (as they are instructed to do regardless of whether they conduct a post-election audit) remain alert for signs of suspiciously high under-voting in high-profile contests and for signs of suspiciously high over-voting rates. Because Wisconsin's voting machines are required to reject over-voted ballots, a review of the chief inspectors' reports will be necessary to notice overvoting problems.
2. Beyond that, the only way to detect alteration of the images is to match the images to the actual paper ballots. Because the DS200 creates no index marks that would allow easy matching of images to ballots, the task would be a time-consuming exercise in matching initials, etc.

Risk #4: Damage or destruction of digital images
Deliberate action or unintentional error could prevent the images from being saved on Election Day. In addition, the digital image files could be corrupted, damaged, or erased in a way that could prevent their use for verification purposes in numerous ways, either deliberately or by accident. If the voter-marked paper ballots have been securely stored and safe, however, damage or destruction of the digital-image files need not prevent verification of the election results.

Security measures to prevent damage or destruction of the digital-image records:

1. Clerks should minimize the window of opportunity for destruction or damage of the digital record by promptly making duplicate copies of the ballot images upon receiving them. The duplicate copies should be promptly distributed to at least a few independent recipients, such as political parties, newspaper, or an independent repository that can prevent undocumented access even by the clerk.
2. Clerks should promptly examine the digital images to check to see whether they appear to be intact, complete and undamaged. If they do appear to have been destroyed or damaged, and the damage cannot positively be attributed to known accident or known inadvertent error, it should be taken as a sign that the election results might have been tampered with, and election results should be verified with a hand count of paper ballots.

Issues related to reliance on a volunteer citizens' audit

Citizens' audits are clearly practicable: Making copies of the digital images is inexpensive, and release of the images to the public presents no risk to the official election records. As a result, citizens should be able easily to obtain copies of full sets of the images after each election. The slide-show verification process is easy and quick, so it is easy to obtain volunteers and citizens' audits could become commonplace.

However, official audits remain preferable to citizens' audits. Chain-of-custody issues limit a citizen audit's credibility in contrast to an official public verification. If detected in an official audit, a miscount could be promptly corrected, building voter and candidate confidence and improving the election officials' reputation. But if detected in a citizens' audit, a miscount would likely be dismissed as the citizens' error, and the miscount would not be corrected. Such events would cause only controversy, diminished confidence, and damage to the election officials' reputation.

However, if elections officials continue to neglect the need to verify the voting machines' accuracy, citizens should step in to perform these audits. With repeated demonstration of the feasibility of these audits, election officials will sooner or later accept the responsibility.

Attachment A:
Verification with paper ballots and with automatically created digital images

Hand counting **Sort, stack, count, count method**	**Slide show with** **Automatically created digital ballot images**
✓ The voter-marked paper ballot is the only guaranteed-accurate record of the voter's intent.	Although editing the digital image needs more sophisticated hacking skills than a simple hack of the tabulation, the only way to guarantee the digital image is true is to locate the matching ballots and compare them. This process negates the time-savings of auditing with digital images.
Even when officials are accommodating, it is hard for observers to view the same ballot that the counter is viewing to see how the counter is tallying it. When officials are not accommodating, they can prevent any meaningful public observation, even when public are allowed to be present. Observation is often boring and unpleasant.	✓ Public observation of the counting process is complete—observers have the same view of the ballots as the official counters. Observers can compare their subtotals to the counters' subtotals as the counters orally report them to the facilitator keeping the overall tally. Observation is fun and interesting.
Pre-audit chain of custody practices require compliance by many people, including minimally trained poll workers. The easiest way to do something is rarely the most secure.	✓ Very few people need to be involved with the pre-audit custody and security of the digital ballot images, and the most secure thing to do with the digital files is often the easiest thing to do.
Tampering with the ballots once they are created requires no specialized skill, but it is harder to access them undetectably.	The images stored on a computer may be easier to access undetectably, but are more technically difficult to alter.
Verifying election results with paper ballots requires unsealing the ballot bags and handling them in a way that protects the integrity of the official record of the election.	✓ If multiple copies of the ballot-image files are made quickly after the election, only reasonable care needs to be taken with any single copy. The open-source software that turns them into a slide show is read-only and does not alter the files themselves.
The better methods of hand-counting paper ballots involve multiple paper-handling tasks—sorting, stacking, counting ballots, and passing stacks of paper between counters.	✓ Paper handling is entirely eliminated, with the exception of a tally sheet kept by the facilitator. Vote-counters need only to view a slide show while using a hand-held counter.
Accurate counting is occasionally impaired by the need to shift one's focus back and forth between the paper ballot and the tally sheet.	✓ Counters can keep their focus steadily on the screen as the ballot images are displayed, and because their hands are free to use counters, fewer tabulating errors are made.
✓ One counter can count multiple contests from one view of each ballot (with a method other than sort, stack, count, count.)	If multiple contests are to be verified, multiple teams need to view the slide show simultaneously; the slide show needs to be repeated; or the counters must use tally sheets like those used in paper-ballot counts.

Obtaining two independently counted totals for each small batch of ballots requires sequential work by two counters—first one counts the batch, then the other counts it, and then they compare totals.	✓ Two or more independently counted totals can be obtained simultaneously for each small batch of ballots, as the counters watch the same slide show, count independently, and then compare totals.
When counters' interpretation of an ambiguously marked ballot differ, it is often difficult to locate the ballot they counted differently and examine it simultaneously.	✓ It is easy to identify the differently-counted vote when the two counters interpret an ambiguous mark differently, by re-running the slide show for a batch of 25 ballots and counting together. Once located, the ballot is easy to view simultaneously to discuss the interpretation.
Sampling ballots is a time-consuming manual process.	✓ After publicly observable random sampling produces a list of images to be retrieved from the files, pulling the randomly selected ballots is quick. Allowing the computer to do the random selection would be possible and even quicker, but would sacrifice transparency.

Attachment B: Unresolved Issues and Questions

Digital ballot images

- Is the resolution (pixels per inch) of the ballot images adjustable? If so, are the ballot images created at the lowest resolution usable?
- What accounts for the missing ballot images in the February and April 2015 elections, and how can election officials ensure that all digital images are created and saved properly in future elections?
- How quickly can security copies of the digital-image files be created following poll-closing, and transferred to multiple independent custodians?
- What procedures are necessary to document the chain of custody of the digital ballot images, and can the downloading of the image files be performed transparently?
- Is there an efficient way with either the DS200 or the Imagecast system to match individual digital images with the original paper ballots to verify the integrity of the digital records?
- The required legal retention period for the digital ballot images needs to be ascertained.

Risk-limiting auditing

- Will county clerks be willing and able to recruit professional-level statistical consultation for sample selection and for determination of whether the results of the sample verified the electronic results?
- The outcomes of statewide races cannot be verified without the cooperation of at least a significant proportion of all counties. The best that a single county can do with a statewide race would be to verify that the outcome *in that county* was identified correctly.
- The pros and cons of sampling individual ballots or sampling entire precincts need to be further explored. At minimum, sampling individual ballots will require counting fewer ballots, but sampling entire precincts has the advantage of providing assessment of the accuracy of specific machines.

Other Audit Procedures

- Unless a clerk is willing to commit to auditing every race, criteria for selecting which races to audit need to be developed. Uncontested races should not be audited, nor should races that will be recounted under s.9.01, Wis. Stats. The top race in every election should always be audited, along with at least one additional randomly selected race. Ideally, races with anomalous results should be audited, but additional work is needed to develop objective criteria for anomalies that will be considered suspicious enough to warrant audit.
- Is the county clerk willing to audit municipal races, or should those be left to the municipality?
- Additional work needs to be done to identify truly transparent methods of random selection.

Endnotes

[i] Douglas W. Jones, and Barbara Simons, *Broken Ballots: Will Your Vote Count?* 2012, CSLI Publications, Stanford, CA, pages 345-346

[ii] An example from Medford, Wisconsin in November 2004: The vendor who set up the machine neglected to provide the machine with instructions to count straight-party-ticket votes, which as a result were not counted. Approximately one-third of the ballots were processed as if they were blank, and no votes were counted. www.wisconsingrassroots.net/_it_happens_all_the_time

[iii] An example from Stoughton, Wisconsin in November 2014: Pre-election testing failed to note that no votes were being counted for a local referendum, a result of a set-up error. www.wisconsingrassroots.net/dust_bunnies_may_be_voting

[iv] An example from the South Bronx, New York City, 2010: Voting machines overheated during Election Day, lost calibration, recorded duplicate votes that invalidated real ones, and disenfranchised approximately one-third of the electorate. http://www.wnyc.org/story/207950-reports-find-machine-errors-led-uncounted-votes-2010/

[v] An example from Stoughton, Wisconsin in November 2014: Paper-lint dust bunnies were determined to be casting phantom votes in one precinct. www.wisconsingrassroots.net/dust_bunnies_may_be_voting

[vi] Lawrence Norden, Eric Lazarus, and the Brennan Center for Justice, *The Machinery of Democracy: Protecting Elections in an Electronic World,* Academy Chicago Publishers, 2007.

[vii] *The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration*, January 2014

[viii] Lawrence Norden, Eric Lazarus, and the Brennan Center for Justice, *The Machinery of Democracy: Protecting Elections in an Electronic World,* Academy Chicago Publishers, 2007, page 212

[ix] *Report on Election Auditing,* by the Election Audits Task Force of the League of Women Voters of the United States, January 2009, page 4

[x] s.7.60(3), Wis. Stats.

[xi] *Wisconsin's Post-election Voting-machine Audit Practices*, Wisconsin Election Integrity Action Team, July 2013 http://bit.ly/1q6KqOx

[xii] www.amstat.org/policy/pdfs/Risk-Limiting_Endorsement.pdf