The League of Women Voters of Dane County presents...

Issues Forum

Protecting Wisconsin Elections

Speakers:
Barry C. Burden, UW-Madison Professor of Political Science and Director, Elections Research Center
Dee J. Hall, Co-founder and Managing Editor, Wisconsin Center for Investigative Journalism
Richard Rydecki, Assistant Administrator, Wisconsin Elections Commission

Wednesday, September 5, 2018
5:30 p.m. Social time with snacks
7:00 p.m. Program with our speakers

Capitol Lakes Grand Hall
333 West Main Street in downtown Madison

The event is free and open to the public.
Free parking in the ramp across the street.
Bring your ticket into Capitol Lakes to get validated.

Planning Committee: Mary Anglim, Karen McKim, Ellen Rosborough, Brook Soltvedt

For more information visit the League’s website at www.lwvdanecounty.org or call 608-232-9447.
Discussion Questions
1. Are you worried about the security of our elections? At what level (local, state, national) are your concerns most urgent? What possible problems are most threatening to you?
2. Basically, we just want our elections to produce correct vote counts by processes in which voters have confidence. What barriers stand in the way of achieving these goals? What risks do you think are most significant?
3. What can citizens and election officials do to minimize these risks?

Action Plans
Below are some ways that you could help improve election security in Wisconsin. These are only suggestions! You need not commit to any of them, and you may have some better ideas. Please let the Program Committee know if and how you would like to follow through.
1. When you vote, watch the process carefully. Ask about anything you don’t understand.
2. Learn how the system works. If you haven’t already done so, take the Voter Education Ambassador training (08/27, 09/05, 10/02 at the City Clerk’s Office) or the LWVDC supplemental training (09/17, 5:45 p.m., Sequoya Library).
3. Volunteer to be a poll worker or Election Observer (more info in the September Bulletin)
4. Observe the pre-election voting machine test conducted by your municipal clerk sometime during the week before each election, to publicly demonstrate that the voting machines are counting votes accurately.
5. Attend the canvass held after the election (4 p.m. on the following Friday, for City of Madison) to observe how questionable ballots and vote-counts are resolved.
6. Attend the September 25 meeting of the Wisconsin Elections Commission where recommendations on audit policies will be discussed. (212 East Washington Ave., 10 a.m. – 4 p.m.) Agenda will be posted at https://elections.wi.gov/about/meetings/2018/September
7. Write to the Wisconsin Elections Commission, to encourage consideration of the LWV recommendations on using the 2018 Omnibus Grant Funding for Election Security Issues.
Remember: you must be pre-authorized to speak on behalf of the League.

LWV Positions

The League of Women Voters believes voting is a fundamental citizen right that must be guaranteed. —Statement of Position on Citizen’s Right to Vote, as Announced by National Board, March 1982.

At the 2004 Convention, the League determined that in order to ensure integrity and voter confidence in elections, the LWVUS supports the implementation of voting systems and procedures that are secure, accurate, recountable and accessible. . . .

At Convention 2006, delegates further clarified this position with a resolution stating that the Citizens’ Right to Vote be interpreted to affirm that the LWVUS supports only voting systems that are designed so that:
They employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter’s intent.

The voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent.

Such verification takes place while the voter is still in the process of voting.

The paper ballot/record is used for audits and recounts.

The vote totals can be verified by an independent hand count of the paper ballot/record.

Routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.

At Convention 2010, delegates added the principle of transparency, so that the League would support voting systems that are secure, accurate, recountable, accessible and transparent.

***

**Guidance to Leagues Regarding 2018 Omnibus Grant Funding for Election Security Issues**

The 2018 Omnibus bill allotted $380 million in grants to be distributed to all states across the country for “improving election security in the states.”

LWVUS recommends that Leagues urge the chief election officer of their state to focus on:

1. **Protect Eligible Voters**
   
   . . .

2. **Enhance Voting Security**
   
   1. Advocate for voting equipment that is secure, accurate, recountable, accessible and transparent. (SARAT)
   
   2. Ensure election officials and administrators are provided with the proper training on cybersecurity measures
   
   3. Institute best practices for ensuring secure elections systems
   
   4. Upgrade systems and address vulnerabilities as identified by the Department of Homeland Security
   
   5. Maintain security of electronic poll books

3. **Ensure Valid Votes are Counted**
   
   1. Encourage election officials to establish risk-limiting audits that use statistical principles to certify election results
   
   2. Provisional ballots should be available and accessible to voters who need them. States should work to reduce the need for provisional ballots while establishing clear standards for counting them following the election
   
   3. Promote “no excuse absentee” voting and establish a process to count all absentee ballots following Election Day
   
   4. Support the expansion of early voting opportunities and ensure that all votes cast in this manner are counted

   * * *


An election audit is a set of procedures designed to investigate whether an election was conducted properly, the voting equipment counted votes accurately, only qualified voters cast ballots in the
election, and the rights of eligible citizens to vote and to experience an efficient and fair voting process were respected.

Defined in this way, the full audit process includes:
(1) Activities typically undertaken before or between elections, such as evaluation of the following:
   the voter registration process, the voting machines to be used, the electronic poll books, and all procedures for running the election;
(2) Evaluation of procedural aspects of the election, such as wait times, polling place worker performance and whether there were appropriate controls on the chain of custody for all election equipment, materials, and ballots; and
(3) Procedures to determine the accuracy of the reported election results themselves. Properly performed audits will guard against both deliberate manipulation of the election and software, hardware or programming problems, since any of these factors could alter the election outcome.

Generally, audits can be divided into two categories:
(1) reviews of processes and procedures that contribute to an orderly and fair election and
(2) verification of the vote counts.

The former can be conducted periodically with follow up examinations implemented to assure that flaws in the process have been corrected, or when there are significant changes in personnel, equipment or election law. Verification of vote counts should occur after every election.

* * *

Background Readings

Notes from the trenches (a round-up of reminders from the Madison City Clerk dated 8-17-18, which shows how transparency can improve election security).

★ Reconciling Number of Voters with Number of Ballots ★
The most important part of closing the polls is documenting that the number of voters matches the number of ballots. Any of you who have staffed or observed a recount understand this. If your last voter slip number matches the number on the tabulator, then you’re already there! However, if the two numbers do not match, the Inspectors’ Statement needs to explain why. This is a job for everyone, not just the Chief Inspector. Remember that at multi-ward polling places, the number on the tabulator should match the sum of the highest voter slip numbers for all the wards.

If there are more ballots in the tabulator than voter slips, you may need to search for the voter who is missing a voter number. This would start with checking that all Election Day Registrations have a voter number, that all used absentee ballot envelopes have a voter number, and checking for voters who signed the poll book but don’t have a number recorded. If that doesn’t work, you may need to actually count how many voters are listed in the poll book (including supplementals) as having voted. If that number is different from the last voter slip, it means there was a mistake (such as the same number being issued to two voters). Use the number of voters you counted and make a note in the Inspectors’ Statement.
One thing we don’t have to check is how many "A"s are in the poll book to
determine the number of absentee ballots. Just count the number of empty
envelopes. This is much faster!

Check the absentee envelopes to make sure they have voter slip numbers and
that the opened ballots are empty: Leopold found their missing ballot this way
and was able to make their numbers match!

★★ Dealing with the Ballots after the polls are closed ★★
We need to look for write-ins on every ballot, even when we are not tallying
registered write-in candidates. This is an opportunity to verify the number of
ballots in the event that the number of voters does not match the number on the	

tabulator. If you think you have more ballots than voters, you can call the Clerk’s
Office for help determining how to check for defective ballots so you can make the
needed adjustment. One polling place was able to fix their numbers by finding a
totally blank ballot without any initials. Obviously, two ballots had stuck together
and the voter didn’t know what to do with the second one, so they put it in the	
	
																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
"WI Elections Commission head says state elections machines are certified and safe," by Lisa Speckhard Pasque, published in the *Capital Times*, July 23, 2018

After Russia’s meddling in the 2016 presidential elections, not everyone is convinced Wisconsin is doing enough for elections security. Russian hackers targeted Wisconsin’s voter registration system, but didn’t successfully access them.

In April, U.S. Rep. Ron Kind wrote a letter stating his concerns that some Wisconsin precincts use voting equipment that could be vulnerable to hacking by “adversarial foreign actors.” He asked Meagan Wolfe, interim administrator for the Wisconsin Elections Commission, to explain how she would make sure that didn’t happen.

“Wisconsinites should know that their vote is secure, and that the state is taking every step possible to ensure our elections never face foreign interference again,” Kind said in a statement.

But according to Wolfe, there's no reason to worry.

The machines are certified and safe, she said on the Sunday political talk show “UpFront with Mike Gousha.” Asked whether her recent briefings at the National Association of State Election Directors would lead her to expect “foreign actors” to try to hack into Wisconsin’s elections, she gave a positive, if somewhat indirect, answer.

“We did not learn any information that changes our course of action as we head into August or November,” she said.

That current course of action includes several efforts to ensure the state's elections are secure: training local elections officials, hiring employees to increase registration security and researching the best methods for post-election audits.

Wolfe replaced Michael Haas after he was ousted based on his previous work for the now-defunct Government Accountability Board. The GAB was dismantled in 2015 by Republicans who cited concerns about bias against them, and a report of the GAB’s handling of its John Doe investigation led some Republican legislators to call for Haas to resign.

Addressing Kind’s concerns, Wolfe said that each piece of Wisconsin voting equipment is certified by both the federal government and the state, and every vote in Wisconsin has a paper trail. As proof of the state’s accuracy, she pointed to the 2016 recount, which resulted in totals that “came out very close to what was tabulated and that did not impact the results at all.” Trump gained 844 votes and Clinton gained 713 votes in the recount.

Wolfe acknowledged that individuals do try to access the state's election system, even now. There are “thousands, if not millions of people, trying to find a way into” the Wisconsin enterprise system, which protects all Wisconsin state agencies, including the election agency.

“But it really is a success story in that there haven’t been any successful attempts to get into that statewide enterprise,” she said. “People try to find a vulnerability in our system and they are not successful.”

Host Mike Gousha asked whether some of those would-be hackers could be trying to get at the information for “nefarious purposes.” Wolfe said they’re “from anywhere and from anyone for
any real purpose, but the important point is just making sure that they’re blocked if they do not have any legitimate business with the state of Wisconsin.”

Unlike some other states, elections in Wisconsin are administered at the municipal, rather than county, level. The state has been focusing on training its 1,853 municipal clerks “making sure they can build on that benefit they have of having a very local connection with their communities” and “are able to really detect anomalies from a very personal place,” Wolfe said.

The state keeps logs of “every single move that’s made on our statewide voter registration system,” Wolfe said. They’re recruiting technology employees to, among other tasks, help automate the monitoring process, thanks to a $7 million federal grant.

“We need to make sure we have people that can analyze those logs, detect anomalies, and also put in flags into our system that help us to identify if something is off kilter, even a little bit,” she said.

While the state already conducts random post-election audits, they’re researching “more robust” processes used by other states. Any proposal to expand the post-election audit process will be brought before the Wisconsin Elections Commission in September, Wolfe said.

* * *

Wisconsin’s election-security story is two very different stories: the Voter-registration system, and the Vote-tabulation system

Below are excerpts from advice for the press by Karen McKim, coordinator of Wisconsin Election Integrity, a volunteer group of citizens that focuses on appropriate use and management of election technology.

<table>
<thead>
<tr>
<th>July 2018</th>
<th>Voter-registration system</th>
<th>Vote-tabulation system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of system</td>
<td>WisVote</td>
<td>One system, the DS200, counts 60-70% of Wisconsin’s votes; ‘ICE’ is the second most popular.</td>
</tr>
<tr>
<td>What does it do?</td>
<td>Records voter registrations; keeps them up to date; prints the poll books you get your name checked off on when you vote, among other election-administration tasks</td>
<td>Reads our ballots, counts our votes, determines who wins our elections.</td>
</tr>
<tr>
<td>Most knowledgeable source for reporters</td>
<td>WEC is your primary source. They know this system inside-out.</td>
<td>Vendors (ES&amp;S, Dominion, Command Central, and Clear Ballot) are your primary source regarding tabulation-system security. Local election officials know only their own local security practices.</td>
</tr>
<tr>
<td>Developer</td>
<td>State of Wisconsin; a collaboration between WEC and Division of Enterprise Technology</td>
<td>Any of several private companies; not always the current vendor</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td><strong>State of Wisconsin</strong></td>
<td><strong>Software is owned by vendors; Hardware is mostly owned by local governments</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>System updates managed by</strong></td>
<td><strong>State of Wisconsin</strong></td>
<td><strong>Four vendors (In a few counties, county officials handle prep for each election's new ballot.)</strong></td>
</tr>
<tr>
<td><strong>Security managed by</strong></td>
<td><strong>State of Wisconsin</strong></td>
<td><strong>Software security:</strong> Vendors, primarily, but local officials right before each election and on Election Day. <strong>Hardware security:</strong> Vendors for their computers; Municipal clerks for voting machines; County officials for central computer.</td>
</tr>
<tr>
<td><strong>General security program</strong></td>
<td><strong>Has all five standard components actively in place: 1) Risk identification; 2) Safeguards; 3) Monitoring to detect events; 4) Response plan; 5) Recovery plan</strong></td>
<td><strong>We have only vendors’ assurances about their practices for risk identification or safeguards. Local officials rely on minimal, informal detection practices, and have no clear plans for response or recovery.</strong></td>
</tr>
<tr>
<td><strong>Who would know if it was hacked?</strong></td>
<td><strong>The State of Wisconsin, specifically the DET and WEC, continuously monitor all cyber activity, with the assistance of the federal DHS. Voters will notice if their registration disappears, but they can re-register at the polls.</strong></td>
<td><strong>We don’t know whether the voting machine companies would know if their software was hacked. Local officials cannot assess their software; hacks wouldn’t show up in the pre-election test; and they don’t use our paper ballots in routine pre-certification audits. Voters can’t tell if their votes were miscounted.</strong></td>
</tr>
<tr>
<td><strong>Has it ever been hacked, in Wisconsin?</strong></td>
<td><strong>State officials know that hackers are continuously trying, and that none have succeeded. US DHS has determined that some attempts came from Russia.</strong></td>
<td><strong>No one knows, because no one examines the software (a copy is in every machine), and no one routinely checks the machines’ Election-Day accuracy against the ballots. There have been electronic miscounts, but none that appear, on their face, to be deliberate.</strong></td>
</tr>
</tbody>
</table>

Here are some things you will hear from Wisconsin's election officials, and what else you should know to form good follow-up questions:

- **"The voting systems are certified."**—Local clerks are generally unfamiliar with the federal certification criteria relating to security (as opposed to criteria regarding accessibility, reliability, etc.); controversies regarding the current value of outdated federal certification standards; and how certification of the design of each system protects the actual machines and software used in the next election. (It doesn’t.) Contact WEC staff for information about state certification criteria relating to system security.
- **"Voting machines are never connected to the Internet."**—1) Election officials have no knowledge of the security or connectivity of the vendor’s computers used to develop voting machines’ software, or
of the security of the software at any time before it comes into their possession before each
election. 2) Polling-place voting machines communicate (either wirelessly or by use of portable
digital media) with a central county elections-management computer. 3) Wisconsin officials do not
inspect these county computers for remote access software, which could have been installed without
their knowledge.

• "Every machine is publicly tested before each election."—Municipal clerks reliably perform voting-
machine tests required by s.5.84, Wis. Stats within 10 days before every election. These tests cannot
detect hacks. Two of the many limitations are: 1) A test done on any other day could not detected a
hack designed to operate only on Election Day. 2) Municipal clerks also typically cast only one vote
for each candidate in the pre-election test, so that if the machine was programmed to 'flip' votes—
that is, county one candidate's votes for another and vice-versa (a predictable programming error, if
not a hack), the pre-election test could not detect it.

• "We verify that the machines counted correctly on Election Night, and double-check during the
canvass."—All Wisconsin jurisdictions routinely check and double-check that ballots were counted
correctly; none routinely check that votes were counted correctly during their canvass. Verifying that
machines counted ballots correctly (but not votes) is equivalent to a bank verifying that an ATM
counted the correct number of transactions, without verifying that the dollars were debited/credited
to the correct accounts.

• "The state orders voting-machine audits."—These voting machine audits, as they were performed
before this year, serve no election-security function. Among other limitations, they occurred only
after November elections in even-numbered years; included only about 100 of the state's 3,500
voting machines, and were completed only after the election results were certified final—too late to
correct any miscounts detected and therefore too late to deter hacking. And those were only a few of
their limitations as a security measure.

The key security question to ask local election officials: "As you sign the certification statement, how
do you know the voting machines credited all the votes to the correct candidates' totals?"

* * *

Learning from Recounts

Ansolabehere, Stephen and Burden, Barry C. and Mayer, Kenneth and Stewart III, Charles, “Learning
from Recounts” (March 14, 2017). MIT Political Science Department Research Paper No. 2017-12. Here
are excerpts from the paper:

In this article, we compare the results of two recent statewide recounts in Wisconsin: the 2016
presidential election and the 2011 state Supreme Court election. In the course of this comparison,
we reach the following conclusions, which are relevant not only in understanding the outcome of
these two cases, but also can help provide guidance for empirically investigating the results of
other recounts.

1. Simply comparing the recounted victory margin with the election night victory margin
significantly understates the degree to which counting errors occurred in the original vote count.

2. As a general matter, aggregated reporting of vote totals, both for the original count and the
recount, undervalue the number of errors made in the original count of ballots.
3. Recounts reveal far more errors in counting ballots for minor-party and write-in candidates than for majority-party candidates.

4. Ballots originally counted by computerized means appear to be at least as accurate as ballots originally counted by hand. . . .

A significant controversy surrounding the 2016 recount in Wisconsin was a claim, expressed with various degrees of certainty, that vote counts produced using computerized equipment — both ballot scanners and direct recording electronic devices — are inherently suspicious and prone to error. . . .

Because the two elections we examine are so different in character, the analysis shows that minor party candidates, write-in candidates and especially “scattered” write-in votes are the most important contributors to errors in vote tabulation. These errors appear to be much more severe that those caused by voting technology or other issues.

We also find that ballots originally counted by computerized means – namely optical scanners and DRE [direct recording electronic] touchscreens – are no less accurate than ballots originally counted by hand, and might in fact be significantly more accurate. . . .

** Risk-Limiting Post-Election Audits 

From Verified Voting Foundation, Inc.

The risk-limiting audit is the gold standard of audits. Risk-limiting means that if the machine-reported count is incorrect, “there is a large, pre-specified chance that the audit will reveal the correct outcome.”

Risk-limiting post-election audits are designed to minimize the size of the audit when the outcome is correct, while with very high probability correcting the outcome, if it is incorrect, by counting all the ballots. The audit continues until there is sufficiently strong statistical evidence that the apparent outcome is right, or until all the ballots have been manually counted. There are several factors that determine the size of the audit. Two are the closeness of the race being audited and the total number of ballots cast in that race.

To understand why, imagine an election with 100,000 votes where the machine results show candidate A beating candidate B by 100 votes. A relatively small number of votes for B that either were incorrectly counted for A or not counted at all could change the result and determine that B was the actual winner. Since a few potentially election-changing discrepancies might not be uncovered by a small audit, a large audit is needed. If, however, the machine results show A beating B by a wide margin of 20,000 votes, but B actually beat A, there would have to be a large number of B votes given to A or not counted at all to change the outcome. Therefore, if only a relatively small number of audit units is examined, it would be highly likely that a large number of wrongly recorded votes would be uncovered. A third factor is the size of the batches for which auditable totals are available. The smaller the batches, the fewer ballots will have to be examined, with individual ballot audits being the most efficient.

The following food example from Philip Stark is instructive. Suppose there are 100 bags of 100 jelly beans each, with some bags having a mixture of flavors and others consisting of a single flavor only. Suppose also that each bag is covered with aluminum foil, so that nobody can tell which is which by
looking at the bags. I love coconut jelly beans and I want to estimate the number of coconut beans in all 100 bags.

One option would be to choose a bag at random, open it, and count all the beans. I could then estimate the total number of coconut beans by multiplying the number in that bag by 100. If I chose a bag that contained only coconut beans, I would estimate that all 10,000 beans were coconut; if the bag consisted of entirely a different flavor, I would estimate that none of the 10,000 beans was coconut; and if I picked a mixed bag, I would assume the ratio of all 10,000 beans was the same as that in the bag I had picked.

Suppose instead the jelly bean bags are all opened by someone else, dumped into a large pot, and stirred well. Suppose I then choose 100 beans at random from the large pot and count the number of coconut beans in that group. The estimate I get in this case will be far more reliable than the estimate I would get by looking at the contents of a single bag, even though in both cases I’m examining 100 jelly beans. To get a similarly reliable estimate on the number of coconut jelly beans in all the bags by drawing individual bags at random, I would have to examine far more bags and count many more jelly beans.

The basic structure of a risk-limiting audit follows the following framework: Hand count ballots until the evidence is strong that the outcome is correct. The number of ballots counted will depend on the errors you observe and the particular method being used. If you see no errors or predominantly errors that, if corrected, help the apparent winner, you need to look at fewer ballots than if you see errors that, if corrected, predominantly help the apparent loser. In sum, the number of ballots that need to be examined depends on the data.

There are also time-saving techniques for doing a risk-limiting audit of all of the ballot races simultaneously, although hand-counting multiple races at once may be significantly harder than counting just one race by the sort and stack method. In 2009 Colorado modified its election law to require risk-limiting audits by 2014.

The following year the American Statistical Association issued a statement endorsing risk-limiting post-election audits. In the same year AB 2023 became law in California. AB 2023 authorizes “the Secretary of State to establish a post-canvass risk-limiting audit pilot program in [five] or more voluntarily participating counties for the purpose of verifying the accuracy of election results.”

* * *

Wisconsin Elections Commission memo, 8/1/2018, County-Level Post-Election Audit Options following Partisan Primary, p. 6, describes the Risk Limiting Audit: “Ballot Polling” Method

Pros: Less labor intensive
Cons: Mathematical calculations involved, may progress to a full hand tally if election result is close

A Risk Limiting Audit (RLA) is a form of audit that is less labor intensive than a full hand tally. This option may be preferable if you have randomly selected a large reporting unit for audit and the margin is not extremely close. We propose using a “ballot polling” RLA method, which takes a random sample or “poll” of the results and compares it to the reported results from the municipality.
The method outlined below is the DiffSum method, which is a simplified version of a ballot polling risk limiting audit. It is a check to confirm that the number of votes in the random sample for the reported winner is greater than the number for the reported loser. The formula accounts for a “risk limit,” which may be chosen. The “risk limit” is the largest chance that the audit will fail to correct an incorrect outcome by not progressing to a full hand tally.

The DiffSum method uses the following formula: \((a - b)^2 > c (a + b)\), where:
- \(A\) = number of votes for winning candidate in the sample,
- \(B\) = number of votes for losing candidate in the sample,
- \(C = 1 + \) number of digits in the total number of votes cast in that reporting unit (if there were 100 votes cast, \(C = 4\), because there are three digits in the total number of votes cast).

Let’s assume in a race for mayor a reporting unit with 100 votes cast was selected for audit, and there are 55 votes for candidate A and 45 for candidate B. Select a sample size based on the number of total ballots in that reporting unit. We recommend a minimum sample size of 10% of total ballots cast or 20 ballots, whichever is greater. Note: the smaller the sample you choose, the greater likelihood additional sampling will be needed. For reporting unit containing 100 ballots, we will sample 20 ballots at a time. Let’s assume 15 ballots are drawn for candidate A and 5 ballots are drawn for candidate B and we choose a margin of error of 15% (and therefore we use 4 as the factor \(C\) because \(1+3=4\)). Risk limit values range anywhere from 0% (a full hand tally) to 20% depending on the type of audit conducted and the desired risk. For the ballot polling method selected, we recommend a risk limit of 15%, as described above.

Again, the equation is \((a - b)^2 > c (a + b)\).

Substituting the actual results, we determine whether \((15 - 5)^2 > 4 (15 + 5)\)?

The result is \(100 > 80\) and the number on the left side of the formula is larger than the one on the right. Accordingly, the reported results of the election are confirmed with a 15% error rate (risk limit). If a smaller risk limit is desired, the formula result will be different and may not confirm the reported election results (see footnote 2, below).

\(^2\)Rivest, Ronald L. DiffSum – A Simple Post-Election Risk-Limiting Audit. 10 May 2018,
\(^3\)The 1 is the number used in this calculation if you want a 15% risk limit/margin of error. Use 2 for a risk limit of 10% or 3 for 6%.