

Guidelines for Ensuring Fair and Accurate Elections

Democracy depends upon citizen vigilance. Use these guidelines to ensure that your local and state officials conduct elections that are fair, honest, and accurately reflect the will of the voters.

The underlying principle of everything:

Transparency is the basis for public confidence.

The more we can see, the more we can trust.

1. You must be able to verify a physical record of your vote before the vote is counted.

You must be able to see a physical record of your vote and verify that it is correct before it is counted. This ballot should be the official, definitive record of your vote. If you vote on a machine, the machines that print the ballots should not be the machines that count the ballots. The ballots should be saved in a secure location after the election. This step provides assurance that, if the machine on which you cast your vote fails to operate correctly or falsifies the results, the error can be detected. The physical ballots must take priority if there is a recount or if electronic and manual recounting give different results.

The process of verifying the separate ballot increases the security of the election system for all voters. This is because there is a very high chance of detecting errors if even half or fewer of the voters actually verify that their ballots are correct.

2. Post vote totals publicly at each polling place, compare totals to central canvass

The vote totals at each polling place, for each candidate and ballot issue, must be made public (e.g., posted physically or on the Internet) shortly after the close of polls, and before the votes are submitted to the central tallying unit. Then the sum of the number of votes at the individual polling places need to be compared to the totals recorded at the central canvass location (county or state). Central processing results can have errors or be falsified—but public posting of vote totals enables citizens to check the accuracy of the central canvass results.

3. Counting the rest of the votes (absentee, vote-by-mail, provisional, etc.)

This refers to absentee, mailed, provisional and write-in ballots, as well as all other ballots which aren't recorded in the conventional fashion. With these ballots, *qualification* becomes an important issue. Qualification is the process of checking that a ballot meets all of the appropriate standards and should be counted. The qualification process is often done out of public view, offering chances for error or fraud. Instead, this step should be viewed by representatives of all parties.

Furthermore, the number of all non-polling place ballots should be counted before they are qualified and opened, and the total number posted along with the counted votes. Then both the qualified and rejected ballots could have a percentage of their number re-qualified by persons different from those who performed the qualification the first time. The results should be the same with regard to qualification and the totals should be the same as the vote totals of those that were qualified. The rejected ballots should also be kept so they are available for requalification if a recount is ordered or the ballot is from a precinct subject to the random manual recount.

Lastly, all of these ballots must be included in the manual audit recount (see below).

4. No identifying information on absentee ballot envelopes

Putting political party or precinct information on the outside of the envelopes makes it very easy to selectively count ballots or even “lose” them before they can be counted!!

5. No outsourcing of ballot sorting and counting

Would you want your vote counted by some private firm, operating outside of public view?

6. High speed vote counting machines need to be thoroughly tested

The high speed ballot scanners that are used in most larger counties to count absentee ballots tend to be hidden from view from the public. These machines are just as vulnerable to errors and fraud as polling place voting machines. Make sure that high speed ballot machines are federally qualified and state certified, and that they are subject to appropriate logic and accuracy (L&A) testing. We understand that this may be difficult. That is all the more reason that it needs to be done—do not let election officials or vendors talk you out of proper security measures. Also do a manual recount of a randomly selected percentage of the ballots to verify their function.

7. Public posting of complete vote totals

Corrections/adjustments should have separate line items so their effect is clearly indicated.

8. Manual auditing: the final step

After each election, a manual recount should be done of a percentage – say 3 to 5 % – of all ballots, including absentee, provisional, and all other special types of ballots. Both the counted and rejected ballots should be sampled for the manual audit. A representative sample is needed to have a high likelihood of discovering fraud or error if it exists. The random selection of ballots to be recounted must be made after all the vote totals from the machines being tested have been made public. The same is true if the ballots of entire precincts are recounted—the precincts should be randomly chosen after the polls are closed and all the vote totals have been posted. The ballots or precincts to be recounted should be chosen in public view and in a way that is considered fair and not predictable in advance. This is a critical step. All sides must agree that the precincts to be manually recounted are chosen truly randomly, and that there was no way that someone could be tipped off in advance as to which precincts were going to be recounted.

9. Voting by Internet or fax: very dangerous!

Subject to possible tampering and a violation of the concept of secret ballots.

10. Don't trust anything or anybody 100%

If anyone says "Trust me" with regard to elections, beware. Public confidence should depend on openness and transparency, not blind trust.

It is important to remember that **all** equipment, including electronic voting machines with "smart cards", central tallying equipment, and even optical scan machines may have problems or be used for vote fraud. Furthermore, we can't rely only on testing. Testing by itself does not guarantee security. Reliability comes from proper design of both the equipment and the system, not from testing. There are simply too many ways to fail. We must design in security rather than trying to discover errors after the fact, and carry out elections in a fashion that the public can understand and in which they can participate.

Written by Tony Smith-Grieco, based on the Commonweal Institute's testimony to the Election Assessment Hearings in Houston, TX, June 2005, developed by Dennis Paull and Katherine Forrest. Please credit the Commonweal Institute as the source if you use this material in any way. We would appreciate your feedback, so we can provide better information to the public.