

A) The most secure way (for a perpetrator) to tamper with votes untraceably is to change votes at the source, DRE. If the perpetrator is successful all documentation, printed and electronic recorded, will reflect the tampered vote. The voters' real intent would be lost. For example, the DRE could be programmed to change one of every "x" votes from candidate A to candidate B when the vote is being cast. The switched vote would be recorded on the printed audit trail and on the electronically recorded vote. Program code could be embedded with rules to make the switch only if 4 conditions are met:

1. The date is the Election Day.
2. The machine is in live voting mode, not test mode.
3. The source of the input is manual, not machine entered "test votes."
4. The voter has not requested a second print out of the audit trail. (In a live situation the voter might be one of the few who actually reads the printed audit trail. He/she might have caught the switched vote on the printed audit trail and assumed that it was his/her error. The voter corrected the vote and requested a second print out.)

B) Refers to I.2.A. Red Teaming. Why should the red team approach the system knowing nothing of DREs software code? One of the greatest vulnerabilities of these systems is from the vendor's software programmers. The premise that the red team knows nothing about the software assumes that the programmers and/or machine manufactures are not the source of the attack. Not a good assumption.

C) Machine code should allow for local elections officials to test under live conditions. Election officials should be allowed to set the machines' date and time, set them in live voting mode and enter any number of transactions. Also election officials should be provided a way to automatically generate votes so that high volume testing could be performed. (Although this is not infallible, see item A condition 3 above, it does offer another level of security.)

D) ALL software changes from the time of certification, whether they are considered version changes or not, should be subject to verifying what code changes were made since the last version. The Secretary of State's future testing procedures should contain automatic identification of code change between versions. This should include changes to update ballot specifics for each county. It would be easy to slip the minor changes to the DRE code when any program change is being introduced. That could compromise an election.

E) Optical readers should determine "voter intent" considering multiple factors. "Voter intent is where a voter marked and did not mark a ballot. Some optical readers judge voter intent based only on the darkness or intensity of the mark on the paper. We used a 6% intensity guideline recommended by the vendor during testing. The machine picked up many false positives. False positives would not be identified in an actual election without a manual count unless it was an over vote. At least one additional criteria should be used, the size of the mark made. The size of the mark could be evaluated as a percent of the space filled or the percentage of the mark that is within the specified marking area.

F) Printers should facilitate reading the audit trail. Some printers are not able to print the entire office and name of candidates that have a long names and descriptions. In these cases part of the name or the office may be truncated. This makes the audit trail confusing and difficult to read. It is unacceptable.